



nemasis[®]
Vulnerability Management Suite

Vulnerability Assessment

User Guide

Product Version: 22.0.1000.124

Document Version: NVA-UG-2201

Copyright © 2021 by MicroWorld Technologies Inc. All rights reserved.

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:	www.nemasisva.com/english/livechat.asp
Printed By:	MicroWorld Technologies Incorporated
Date:	August, 2021

Content

Introduction	6
Scope and Purpose	6
Supported Platforms/Browsers	7
Login	8
Dashboard	10
Add a Dashboard	11
Add a Display to Dashboard	11
Delete a Display from Dashboard	13
Remove a Dashboard display	13
Scan	16
Task	16
Add a Task	17
Compare Task Reports	22
Quick Task	23
Add a Quick Task	23
Export a Task Report	25
Advanced Quick Task	26
Add an Advanced Quick Task	26
Delete a Task	28
Clone a Task	29
Edit a Task	29
Stop a Task	30
Resume a Task	30
Assets	31
Host	31
Operating Systems	31
Task Results	32
Task Dashboard	32
Results	33
Vulnerabilities	34
Reports	35
Delete a Task Report	35
Security Info	36
Scan Plugins	36
CVE	37
CPE	38
OVAL Definitions	39
Configurations	40
Targets	40

Add a Target.....	41
Delete a Target.....	46
Clone a Target.....	46
Edit a Target.....	47
Port Lists.....	48
Add a Port List.....	49
Delete a Port List.....	51
Clone a Port List.....	51
Edit a Port List.....	52
Credentials.....	53
Add a Credential.....	54
Delete a Credential.....	57
Clone a Credential.....	58
Edit a Credential.....	58
Alerts.....	59
Add an Alert.....	60
Delete an Alert.....	68
Clone an Alert.....	68
Edit an Alert.....	69
Scan Configs.....	71
Add a Scan Config.....	74
Delete a Scan Config.....	75
Clone a Scan Config.....	76
Edit a Scan Config.....	76
Schedules.....	77
Add a Schedule.....	78
Delete a Schedule.....	80
Clone a Schedule.....	80
Edit a Schedule.....	81
Scanners.....	82
Add a Scanner.....	83
Delete a Scanner.....	85
Clone a Scanner.....	85
Edit a Scanner.....	86
False Positives.....	87
Add a False Positive.....	88
Delete a False Positive.....	89
Asset Tagging.....	90
Add an Asset Tag.....	90
Delete an Asset Tag.....	91
SMTP.....	92

Administration.....	93
Users.....	93
Add a User	94
Delete a User.....	95
Clone a User	96
Edit a User	96
Roles	97
Secure LDAP (LDAPS)	98
Add an LDAP.....	99
Customize Header.....	101
Add a Custom Header	101
Remove the Custom Header	102
User Settings.....	103
Scan and Dashboard Settings	103
Timezone	104
Passive Scanner.....	105
Settings.....	106
Activity Monitor	108
Host.....	109
Country.....	111
Vulnerabilities	113
License	115
Enter Subscription Key	116
Buy Now	116
Manage Instance.....	117
Two-Factor Authentication (2FA).....	118
Enable 2FA login	119
Enable 2FA login for added users	122
Disable 2FA login	123
Import & Export.....	125
Export an Instance.....	125
Import an Instance	126
Offline Updates.....	127
Upload Offline Updates	127
System Information.....	128
Whitelisted IP	129
Add a Whitelisted IP	129
Delete an IP	130
Audit Trail.....	131
Search audit trail by IP address	131
Help & Support.....	133

Feedback	133
Support Request.....	133
Contact Us.....	134
Chat Support.....	134
Email Support	134

Introduction

The Nemasis is a Vulnerability Management Suite that detects vulnerabilities in your network and suggests accurate solution to fix it. It assists you in managing your organization's overall governance, risk and compliance with regulations. The Nemasis is designed to keep you and your organization safe from the cybersecurity threats and ensure you are protected 24/7. Below we have mentioned key features of Nemasis:

- Scan endpoints connected across the network for vulnerabilities.
- Report vulnerabilities found and suggest accurate solutions to fix them.
- Monitor security status of the organization endpoints.
- Create and manage scan tasks for endpoints.
- Send customized alerts and reports of scan tasks according to your preferences.
- Monitor network continuously with Passive Vulnerability Scanner.
- Display information about open ports, malicious applications, or running services.

As the technology is evolving, so are the threats. But with Nemasis at your hand, we are sure that your organization operations will run fluid smooth. The Nemasis follows 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 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.

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 console. Please note that this User Guide does not cover the installation process. If you want to read installation process, download the [Installation Guide](#).

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
- Microsoft Edge
- Safari

Login

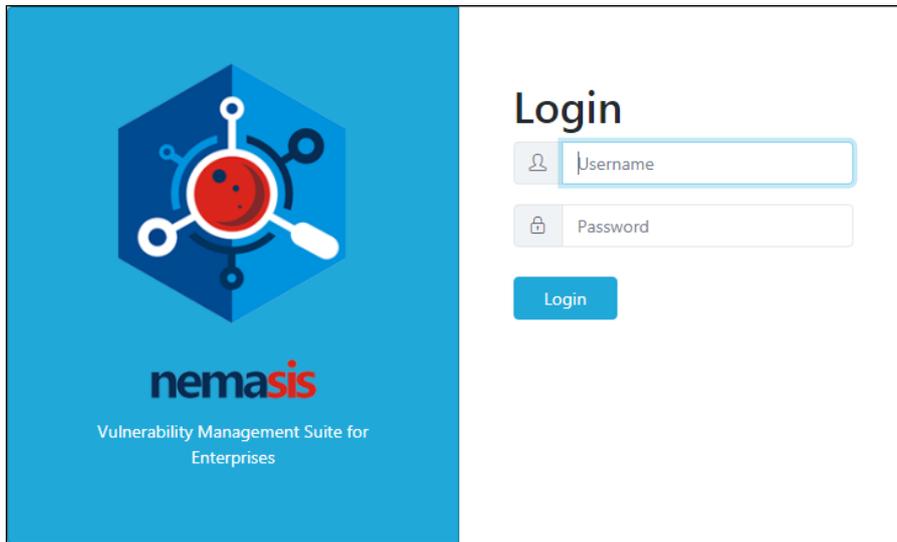
To log in to the Nemasis console,

1. Open a web browser.
2. Enter the URL – IP address of the Nemasis installed system:10442

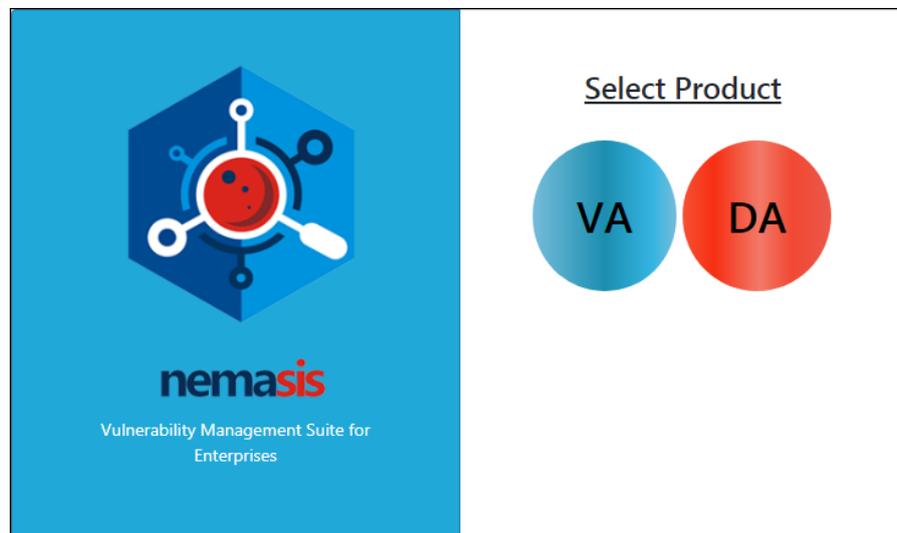
TIP

If the Nemasis installed system's IP address is 192.168.0.1, then the URL will be – <https://192.168.0.1:10442>

Nemasis console login page appears.

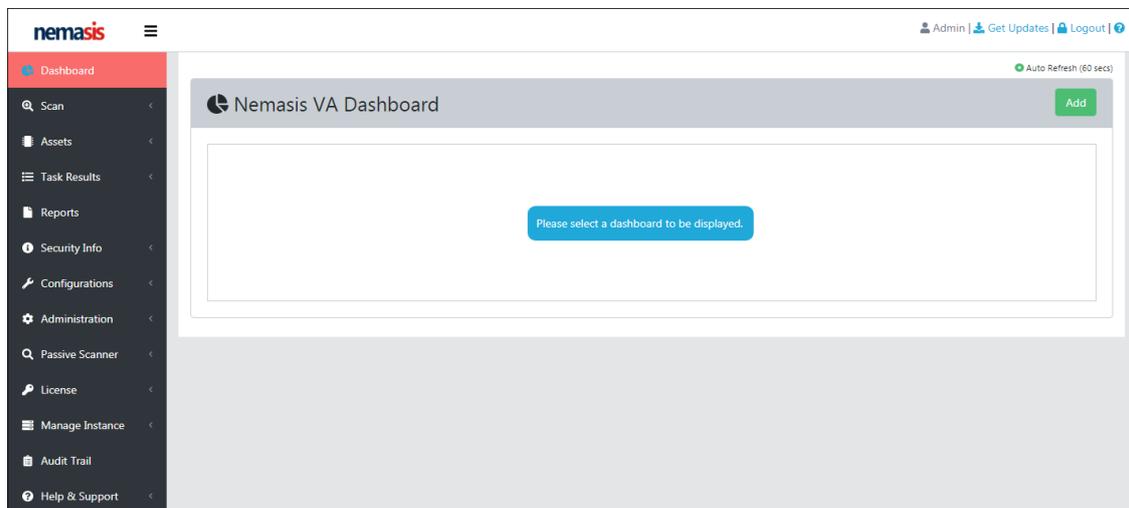


3. Enter the default login credentials.
Username – admin
Password – admin
4. Click **Login**.
Select Product screen appears.



5. Click **VA**.

After logging in to the Nemasis, following screen appears.

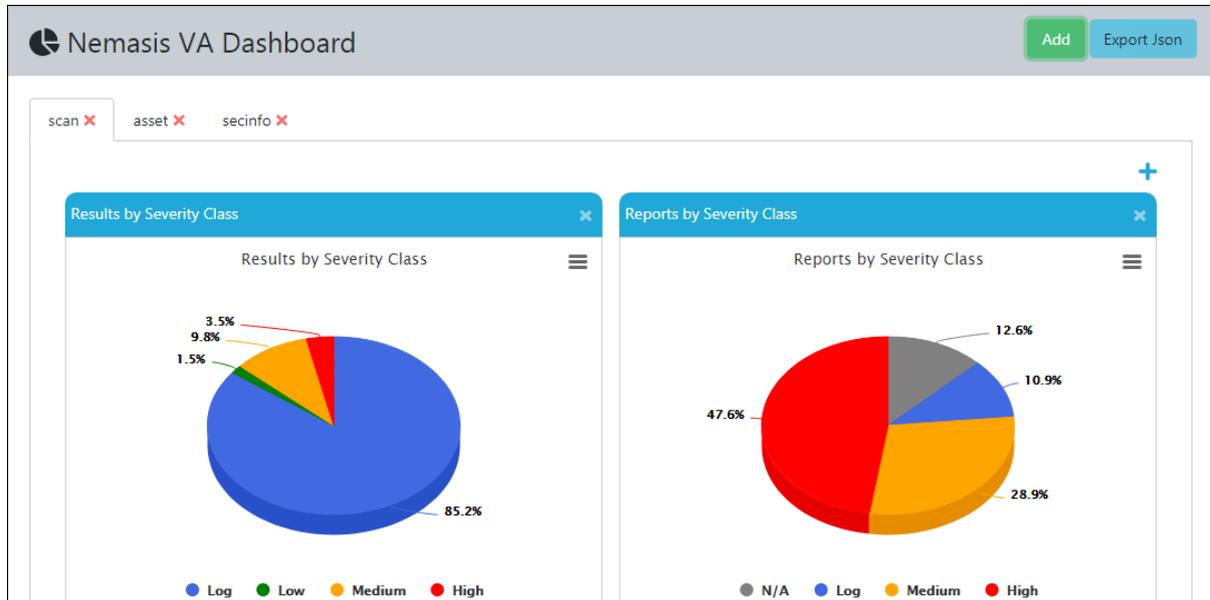


The console tree on the left side consists following modules:

- **Dashboard**
- **Scan**
- **Assets**
- **Task Results**
- **Reports**
- **Security Info**
- **Configurations**
- **Administration**
- **Passive Scanner**
- **License**
- **Manage Instance**
- **Audit Trail**
- **Help & Support**

Dashboard

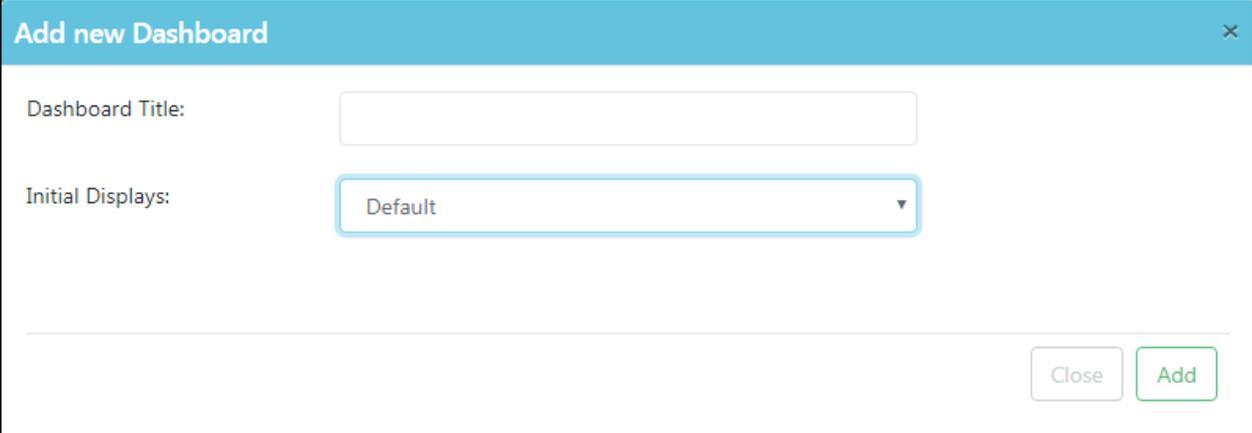
The Dashboard module displays overall scan results in interactive pie, bar and line charts. You can view the specific information by clicking in pie and bar charts.



Add a Dashboard

To add a Dashboard,

1. In the upper right corner, click **Add**.
Add new Dashboard window appears.

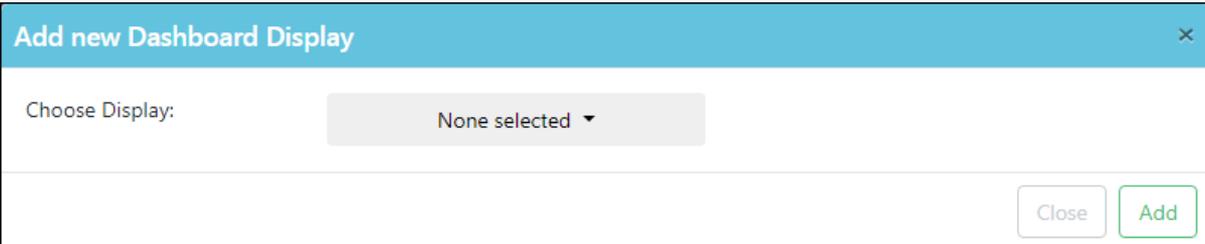


2. Enter a name in the **Dashboard Title** box.
3. Click **Initial Displays** drop-down, select the preferred display and then click **Add**.
The new Dashboard display gets added to Dashboard.

Add a Display to Dashboard

To add a display to Dashboard,

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



2. Click **Choose Display** drop-down, select the required display and then click **Add**.
The new Dashboard display gets added to Dashboard.

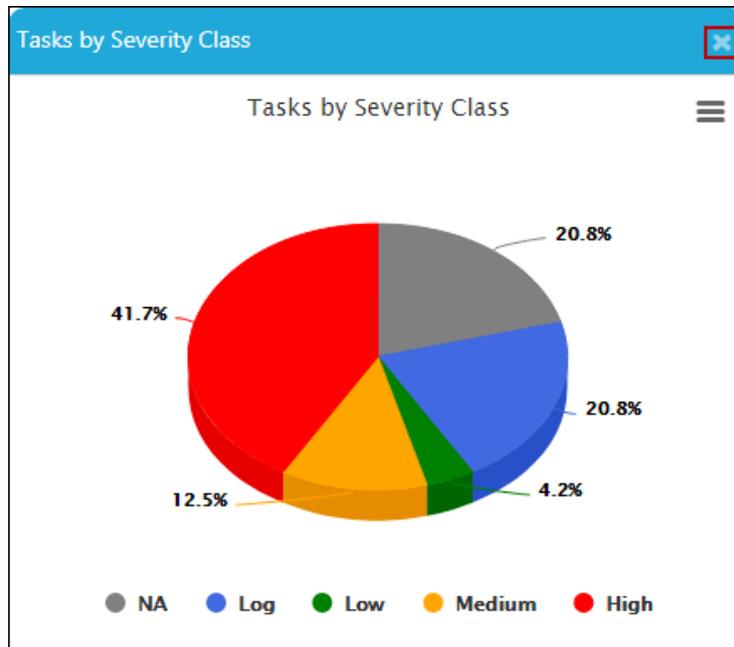
Following displays can be added to Dashboard:

- Tasks by Status
- Results 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
- 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

Delete a Display from Dashboard

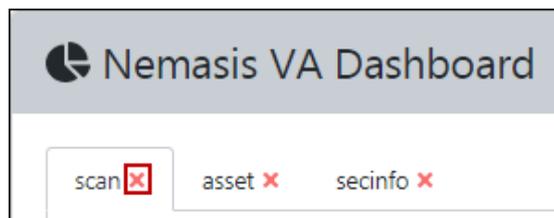
To delete a display from Dashboard, in the display, click .



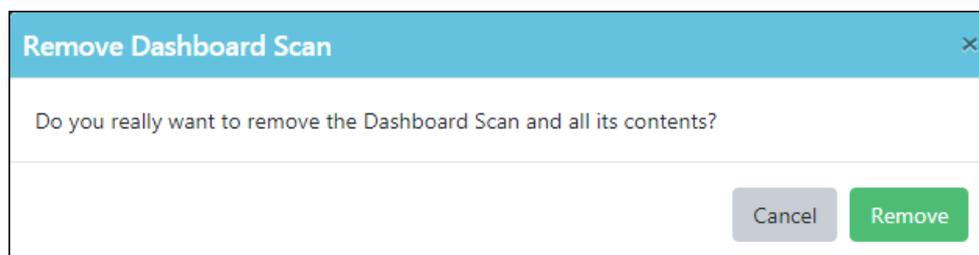
The display gets deleted.

Remove a Dashboard display

1. To remove a Dashboard display, click .

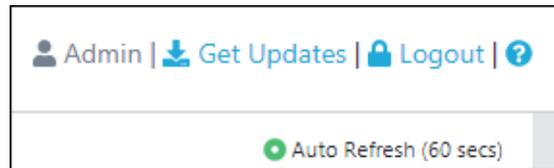


A confirmation prompt appears.



2. Click **Remove**.
The Dashboard display gets removed.

In the top right corner, there are additional options.



Get Updates

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

Logout

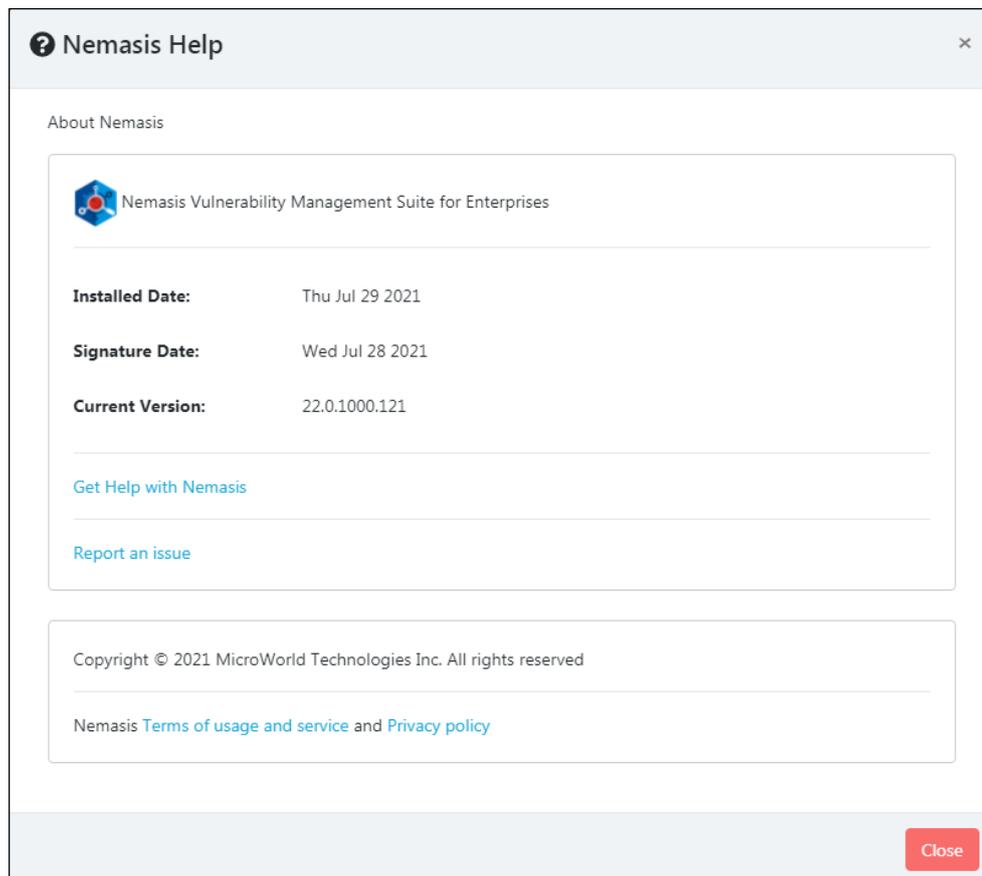
Clicking **Logout** will log you out of the Nemasis console.

Auto Refresh

The Dashboard is refreshed automatically after 60 seconds.

Nemasis Help

Clicking  displays the Nemasis Help pop-up.



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

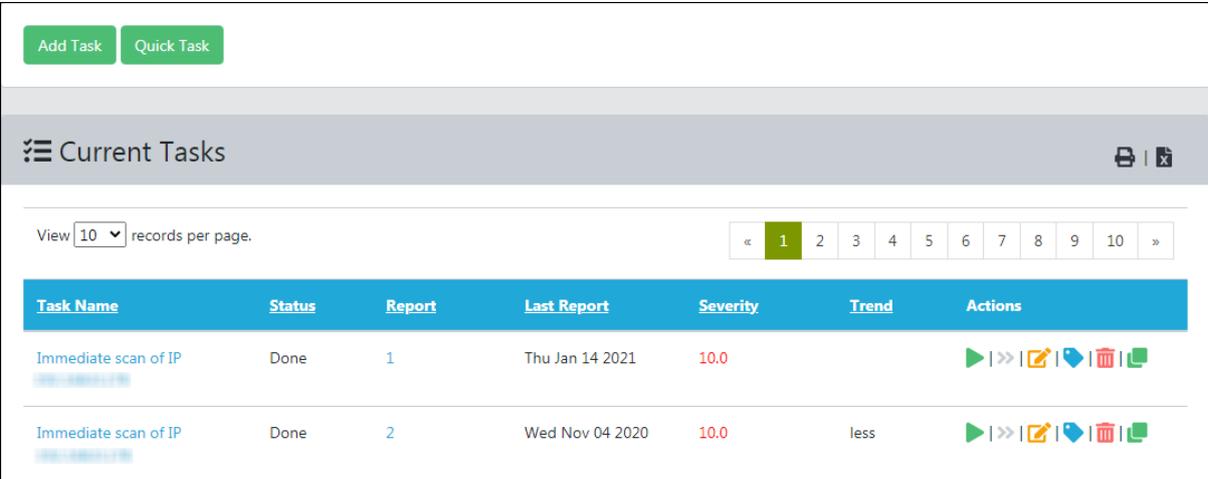
Scan

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

Task

The Task submodule displays the list of tasks.

The **Status** column displays whether a task is **In Progress** or **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
Immediate scan of IP View Report	Done	1	Thu Jan 14 2021	10.0		
Immediate scan of IP View Report	Done	2	Wed Nov 04 2020	10.0	less	

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 after a task is rerun. An overall score is matched of latest scan with the last scan, irrespective of the vulnerabilities discovered. The Trend column displays following parameters:

Down – Less vulnerabilities found compared to the last scan.

Up – More vulnerabilities found compared to the last scan.

Same – Similar vulnerabilities found compared to the last scan.

Add a Task

To add a Task,

1. Go to **Scan > Task**.
2. Click **Add Task**.
Add Task form appears.

Add Task

Basic Target and Alerts Scanner and Config

Name*:

Description:

Add Result to Asset:

Alterable Task:

Min. Detection Threshold*: %

Auto Delete Reports:

Do not automatically delete reports

Automatically delete oldest reports but always keep newest

Add Task

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

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

Basic

The Basic tab is explained below:

1. Enter the task name.
2. Enter the task description.

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. To enable/disable adding result to asset, click the toggle.

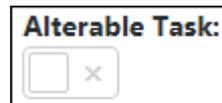


3. Select configuration for **Add Result to Asset**.

Alterable Task

This feature lets you modify a task even if the report for the same task is already generated. To make the task alterable, click the toggle.

 NOTE	If the tasks are altered, there will be no consistency amongst task reports.
----------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------



4. Select configuration for **Alterable Task**.
5. In the **Min Detection Threshold box**, enter quality for the addition of the results to the asset database.

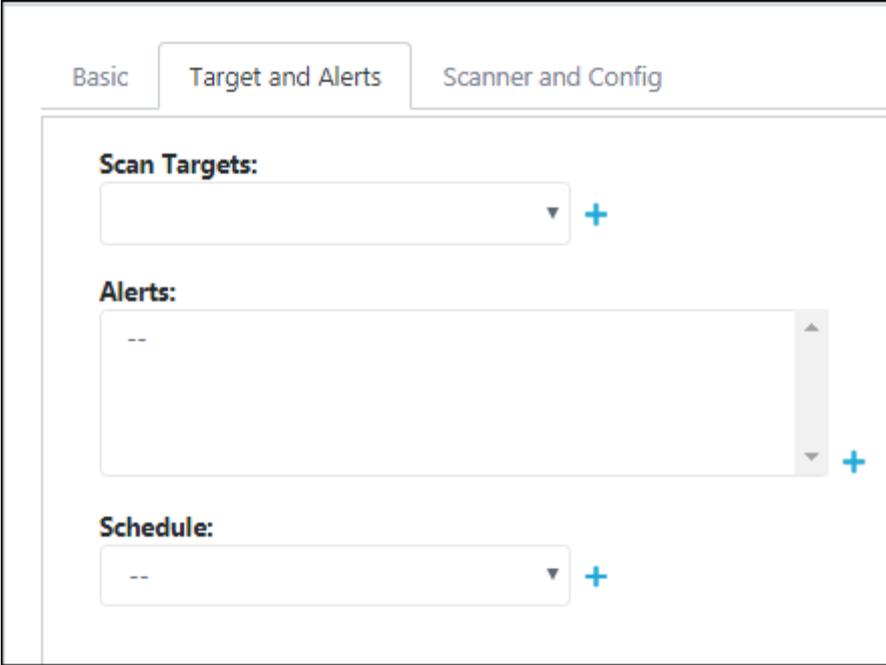
Auto Delete reports

- **Do not automatically delete reports** – When this option is selected, Nemasis will not auto-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** – When this option is selected, you enable Nemasis 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.

6. Select the preferred option for **Auto Delete Reports**.

Targets and Alerts

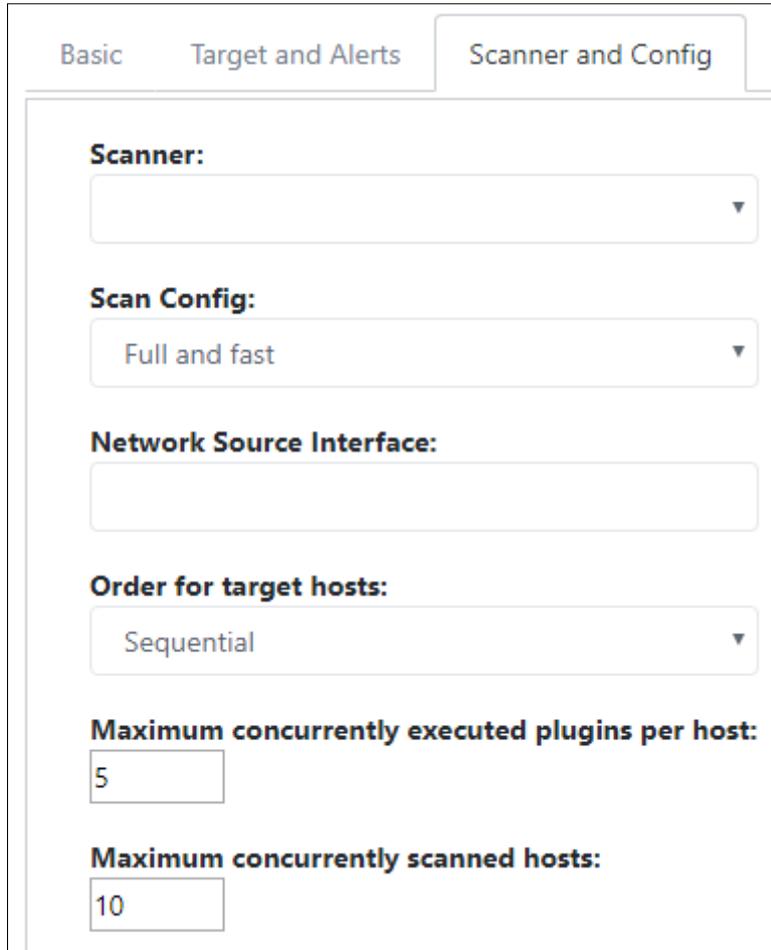
The Targets and Alerts tab is explained below.



7. Click the **Scan Targets** drop-down and select the appropriate Target. To add a new Target from the tab, click **+**.
Learn more about Targets by clicking [here](#).
8. Select the appropriate Alert from the **Alerts** list. To add a new alert from the tab, click **+**.
Learn more about Alerts by clicking [here](#).
9. Click the **Schedule** drop-down 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.



The screenshot shows a configuration window with three tabs: 'Basic', 'Target and Alerts', and 'Scanner and Config'. The 'Scanner and Config' tab is active. It contains the following fields:

- Scanner:** A drop-down menu.
- Scan Config:** A drop-down menu with 'Full and fast' selected.
- Network Source Interface:** A text input field.
- Order for target hosts:** A drop-down menu with 'Sequential' selected.
- Maximum concurrently executed plugins per host:** A text input field with '5' entered.
- Maximum concurrently scanned hosts:** A text input field with '10' entered.

10. Click the **Scanner** drop-down and select the appropriate Scanner.
Learn more about Scanner by clicking [here](#).
11. Click the **Scan Config** drop-down and select the appropriate Scan Config.
Learn more about Scan Config by clicking [here](#).
12. Enter the **Network Source Interface** of the Nemasis for the scan.

Order for target hosts

You can select the search type for a specified network area. Following options are available:

- Sequential
- Random
- Reverse

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

13. Click the **Order for target hosts** drop-down and select the preferred option.

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 and maximum concurrently scanned hosts. The default number of Scan Plugins is chosen with utmost care. If a target is scanned with more than default number of Scan Plugins or a scan is run for numerous targets at the same time, then the target systems or the network or the Nemasis appliance may face a negative impact.

14. Click **Add Task**.

The Task gets added in Current Tasks list.

Compare Task Reports

To compare Task Reports after a Task is rerun,

1. Click the numerical in **Reports** column.
Taskwise Reports page appears. When comparing Task Reports, the first selection is the **Base Report**, while the next selection is the **Compared Report**.

Taskwise Reports

View records per page.

Date	Status	Task	Severity	High	Medium	Low	Log	Actions
<input type="checkbox"/> Nov 04 2020 12:37 PM	Done	Immediate scan of IP [REDACTED]	10.0	1	4	1	27	<input type="button" value="🗑"/>
<input type="checkbox"/> Oct 31 2020 03:53 PM	Done	Immediate scan of IP [REDACTED]	10.0	3	14	1	27	<input type="button" value="🗑"/>

2. Ensure the correct selection sequence and then in the upper right corner, click **Compare**.
Report Compare window appears.

Report Compare: Immediate scan of IP [REDACTED]
×

Base Report: Nov 04 2020 12:37 PM

Compared Report: Oct 31 2020 03:53 PM

Vulnerability	Severity	Detection Threshold	Host	Protocol	Status
Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)	10.0	99%	[REDACTED]	3389/tcp	Same
Apache HTTP Server 2.4.20 - 2.4.39 Multiple Vulnerabilities (Windows)	7.8	80%	[REDACTED]	2221/tcp	New
Apache HTTP Server 2.4.32 < 2.4.44 mod_proxy_uwsgi Buffer Overflow Vulnerability (Windows)	7.5	80%	[REDACTED]	2221/tcp	New
Apache HTTP Server Memory Access Vulnerability (Windows)	6.4	80%	[REDACTED]	2221/tcp	New


NOTE

At a time, only two reports can be compared.

Quick Task

The Quick Task lets you run a scan task instantly.

★ Quick Task

IP Address :

The default address is either your computer or network gateway.
Nemasis 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

Add a Quick Task

To add a Quick Task,

1. Go to **Scan > Quick Task**.
2. In the IP address box, enter the IP address of the target system.
3. Click **Add Quick Task**.

The Quick Task gets added to the Current Tasks list and Nemasis runs the task immediately.

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
Immediate scan of IP	Running (1%)	2	Thu Jan 14 2021	10.0		

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

- Start Task
- Stop Task
- Resume Task
- Edit Task
- Delete Task
- View Asset Tag for Task
- Clone Task
- Task is scheduled

The **Report** column displays the number of reports generated for the task. You can view the report while the scan task is in progress and after it gets completed, by clicking the numerical.

The **Severity** column displays criticality of any vulnerability detected. Clicking the numerical in **High, Medium, Low** and **Log** column displays only Results tab from the report.

Taskwise Reports

 Compare

View records per page.

Date	Status	Task	Severity	High	Medium	Low	Log	Actions
<input type="checkbox"/> Nov 04 2020 12:37 PM	Done	Immediate scan of IP [REDACTED]	10.0	1	4	1	27	<input type="button" value="🗑"/>
<input type="checkbox"/> Oct 31 2020 03:53 PM	Done	Immediate scan of IP [REDACTED]	10.0	3	14	1	27	<input type="button" value="🗑"/>

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

Report: Nov 04 2020 12:37 PM(Immediate scan of IP [REDACTED])

Info
Results
Hosts
Ports
Applications
Operating Systems
CVEs
TLS Certs

Search By

1 - 10 / 33

Vulnerability	Severity	Detection Threshold	IP	Protocol	Created
Apache HTTP/Web Server Detection (HTTP)	0.0	80%	[REDACTED]	2221/tcp	Wed Nov 04 2020 12:43:09

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

Export a Task Report

The Task Report contains Summary, Vulnerability Detected, Solution, Vulnerability Insight, Detection Method and CVE references. It can be exported in following formats:

- PDF
- Excel
- Excel Vulnerability wise
- XML
- TXT
- PCI-DSS
- PCI-DSS (Executive)

To export a Task Report,

1. In the upper right corner, click **Export**.
Export window appears.



The screenshot shows a dialog box titled "Export" with a close button (X) in the top right corner. Below the title bar, there is a label "Report Format:" followed by a dropdown menu currently displaying "PDF". At the bottom right of the dialog, there are two buttons: "Cancel" and "OK".

2. Click the drop-down and select the preferred format.
3. Click **OK**.
The Task Report gets exported.

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 :

Target IPs :

Start Options :

Start Immediately

Schedule for Later

Do Not Start Automatically

SSH Credential : on

SMB Credential :

ESXi Credential :

Send Email to :

Add an Advanced Quick Task

To add an Advanced Quick Task,

1. Go to **Task > Advanced Quick Task**.
2. Enter a name for the Task.
3. Click the **Scan Config** drop-down and select the preferred scan configuration.

Target IPs

You can enter the IP address in the box with 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
4. Enter the IP address or import a list of IP addresses in **Target IPs** box.

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 preferred date, time and region.
- **Do Not Start Automatically** – Select this option to start the task manually.

5. Select the preferred Task Start option.

SSH Credential

If the target system runs on Linux or UNIX, click this drop-down and select the appropriate credential.

SMB Credential

If the target system runs on Microsoft Windows, click this drop-down and select the appropriate credential.

ESXi Credential

If the target system is a VMware ESXi system, click this drop-down and select the appropriate credential.

Learn more about Credentials, by clicking [here](#).

6. Select the appropriate credential.
7. Enter the report recipient's email ID in **Send Email to** box.
8. After filling all the boxes, click **Add Advanced Quick Task**.
The Advanced Quick Task gets added to the Current Tasks list.

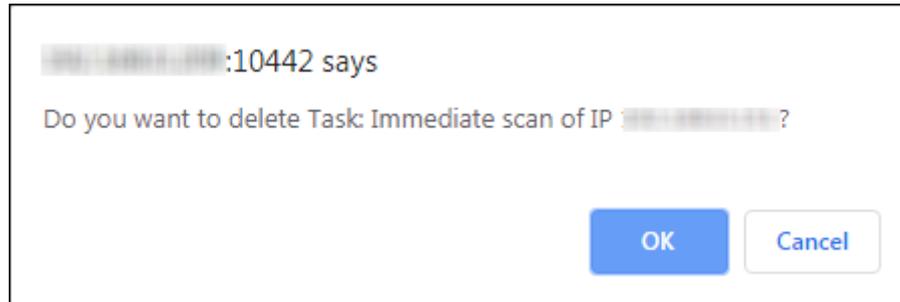
In the upper right corner there are two buttons available.

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

Delete a Task

To delete a Task,

1. Go to **Scan > Task**.
2. In the Current Tasks screen, in the Actions column, click .
A confirmation prompt appears.



3. Click **OK**. The Task gets deleted.

Clone a Task

To clone a Task,

- Go to **Scan > Task**.
- In the Current Tasks screen, in the Action column, click . The Task gets cloned.

Edit a Task

To edit a Task,

1. Go to **Scan > Task**.
2. In the Current Tasks screen, in the Actions column, click . Edit Task window appears.

Edit Task

Basic Target and Alerts Scanner and Config

Name*:

Description:

Add Result to Asset:

Alterable Task:

Min. Detection Threshold*: %

Auto Delete Reports:

Do not automatically delete reports

Automatically delete oldest reports but always keep newest

Update Task

3. Make the necessary changes and then click **Update Task**. The Task gets edited and updated.

Stop a Task

To stop a running Task,

1. Go to **Scan > Task**.
2. In the Current Tasks screen, in the Actions column, click .
The running Task gets stopped.

Resume a Task

To resume a stopped Task,

1. Go to **Scan > Task**.
2. In the Current Tasks screen, in the Actions column, click .
The stopped Task resumes.



The icon  will change to  only if an in progress task is stopped. If you resume a stopped task, the Nemasis will exclude the scanned IP addresses.

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.

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	Actions
			Windows Server 2003 3790 Service Pack 2	0.0	Tue Jan 12 2021	
			Windows Server 2008 R2 Standard 7601 Service Pack 1	10.0	Wed Sep 23 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 4 >

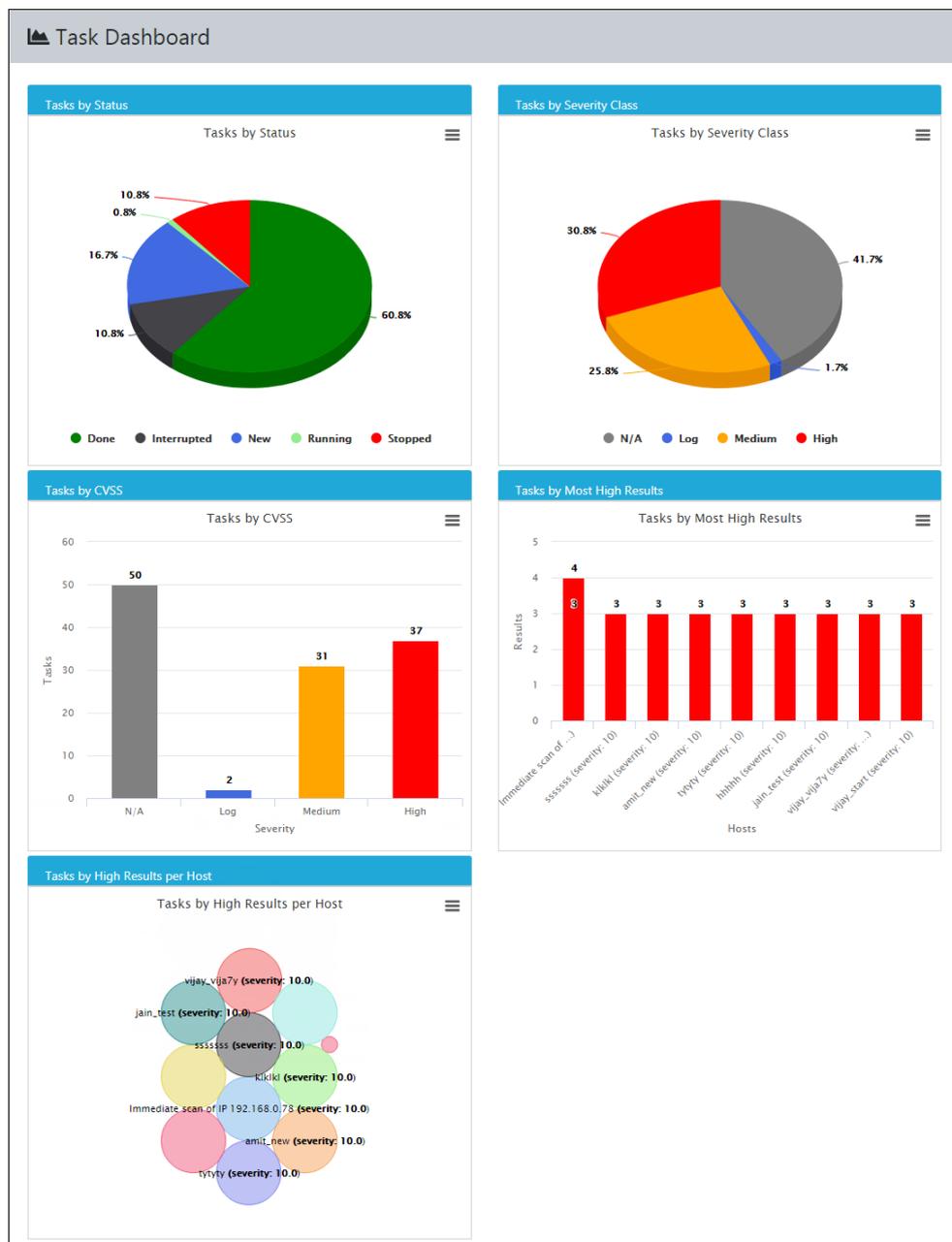
Name	Severity			Host	Modified	Actions
	Latest	Highest	Average			
o:canonical:ubuntu_linux	5.0	5.0	5.0	1	Fri Jul 17 2020	
o:canonical:ubuntu_linux:14.04	5.0	5.0	5.0	1	Fri Jul 17 2020	
o:canonical:ubuntu_linux:16.04	5.0	5.0	5.0	1	Fri Jul 17 2020	

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.

Task Results- Cumulative Search Filter [→](#) [✕](#) [?](#) [🖨](#) [📄](#)

View records per page. « **1** 2 3 4 5 6 7 8 9 10 »

Vulnerability	Solution Type	Detection Threshold	Host IP	Host Name	Protocol	Severity	Detection
Anti-Scanner Defenses (HTTP)	Web application abuses	70	[REDACTED]	[REDACTED]	8081/tcp	0.0	Thu Mar 19 2020
Anti-Scanner Defenses (HTTP)	Web application abuses	70	[REDACTED]	[REDACTED]	8000/tcp	0.0	Thu Jul 02 2020
Anti-Scanner Defenses (HTTP)	Web application abuses	70	[REDACTED]	[REDACTED]	8000/tcp	0.0	Thu Jul 02 2020
Anti-Scanner Defenses (HTTP)	Web application abuses	70	[REDACTED]	[REDACTED]	8000/tcp	0.0	Thu Jul 02 2020

Search Filter

You can filter the displayed information by using 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 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 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

→
✕
i
🖨
📄

View records per page.

<
1
2
3
4
5
6
7
8
9
10
>

Name	Oldest Result	Newest Result	Severity	Detection Threshold	Results	Hosts
Anti-Scanner Defenses (HTTP)	Thu Mar 19 2020	Tue Jul 14 2020	0.0	70	17	2
AnyDesk Version Detection (Windows)	Thu Jan 21 2021	Thu Jan 21 2021	0.0	97	1	1
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	Thu Jul 16 2020	Fri Aug 07 2020	4.3	99	4	2
Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Windows)	Thu Jul 16 2020	Thu Jul 16 2020	5.0	80	1	1

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 **Results** tab, additional information about vulnerability is displayed containing its summary and detection result. The report can be exported in PDF, Excel, XML, TXT and PCI-DSS (PDF) formats.

Taskwise Reports

View records per page.

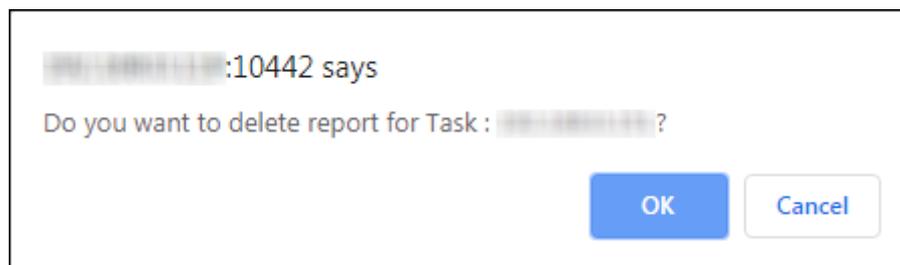
« 1 2 3 4 5 6 7 8 9 10 »

Date	Status	Task	Severity	High	Medium	Low	Log	Actions
Jan 21 2021 01:17 PM	Running (28%)	ESCAN_TASK	10.0	3	8	1	32	
Jan 21 2021 12:56 PM	Done	ESCAN_TASK	10.0	7	12	2	48	
Jan 21 2021 12:40 PM	Stopped at 1%	Immediate scan of IP [REDACTED]	0.0	0	0	0	2	
Jan 14 2021 12:16 PM	Done	Immediate scan of IP [REDACTED]	10.0	3	3	1	26	
Nov 04 2020 12:37 PM	Done	Immediate scan of IP [REDACTED]	10.0	1	4	1	27	

Delete a Task Report

To delete a Task Report,

1. Go to **Reports**.
2. In the Actions column, click .
A confirmation prompt appears.



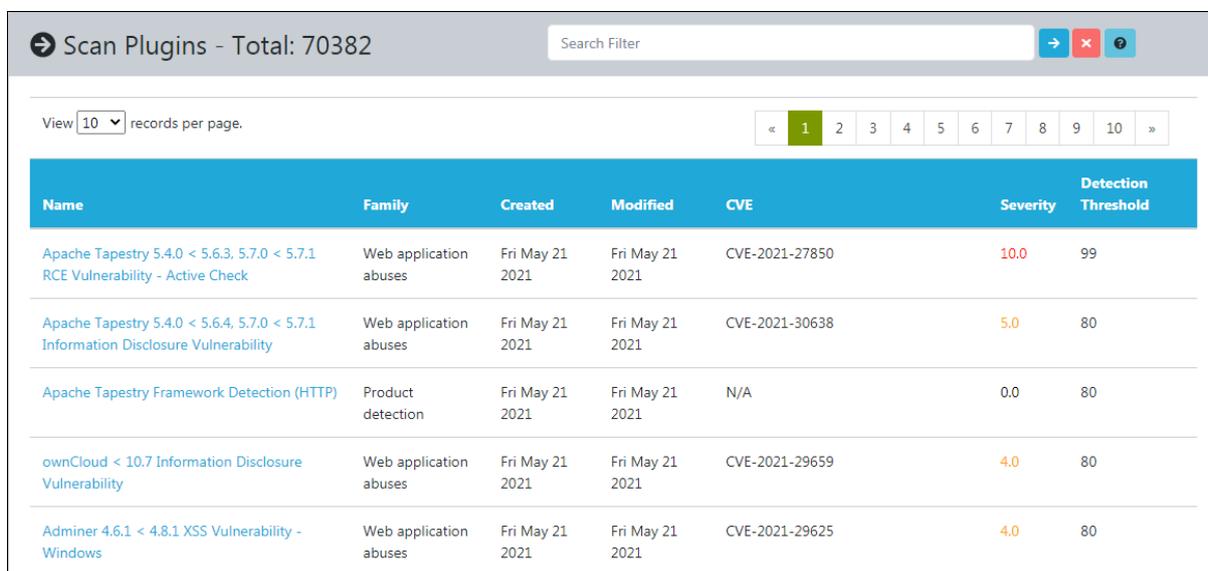
3. Click **OK**.
The report gets deleted.

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 run by Nemasis to scan a system for potential vulnerabilities. You can update Scan Plugins, run them against an endpoint and identify the network vulnerabilities. After the scanning is completed, the Nemasis displays accurate solutions to patch vulnerabilities. After the scan is completed.



Scan Plugins - Total: 70382

Search Filter

View 10 records per page.

< 1 2 3 4 5 6 7 8 9 10 >

Name	Family	Created	Modified	CVE	Severity	Detection Threshold
Apache Tapestry 5.4.0 < 5.6.3, 5.7.0 < 5.7.1 RCE Vulnerability - Active Check	Web application abuses	Fri May 21 2021	Fri May 21 2021	CVE-2021-27850	10.0	99
Apache Tapestry 5.4.0 < 5.6.4, 5.7.0 < 5.7.1 Information Disclosure Vulnerability	Web application abuses	Fri May 21 2021	Fri May 21 2021	CVE-2021-30638	5.0	80
Apache Tapestry Framework Detection (HTTP)	Product detection	Fri May 21 2021	Fri May 21 2021	N/A	0.0	80
ownCloud < 10.7 Information Disclosure Vulnerability	Web application abuses	Fri May 21 2021	Fri May 21 2021	CVE-2021-29659	4.0	80
Adminer 4.6.1 < 4.8.1 XSS Vulnerability - Windows	Web application abuses	Fri May 21 2021	Fri May 21 2021	CVE-2021-29625	4.0	80

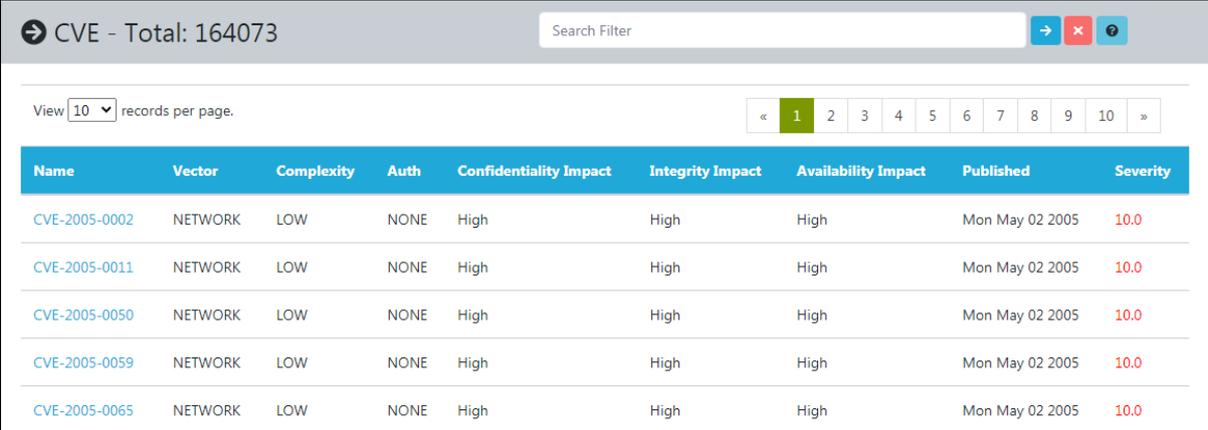
You can filter the displayed information to find a specific result by using following filter tags:

- name
- family
- severity

Clicking a Scan Plugin 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 grants an attacker direct access to a network or system. And, **Exposure** is a flaw in software code that grants an attacker indirect access to a network or system. Nemasis has a database of vulnerabilities and provides solution for the same.



The screenshot shows a web interface for the CVE database. At the top, it displays 'CVE - Total: 164073' and a search filter box. Below the search bar, there is a pagination control showing 'View 10 records per page.' and a page number selector with '1' highlighted. The main content is a table with the following columns: Name, Vector, Complexity, Auth, Confidentiality Impact, Integrity Impact, Availability Impact, Published, and Severity. The table lists five entries, all with a severity of 10.0 and a publication date of Mon May 02 2005.

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

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

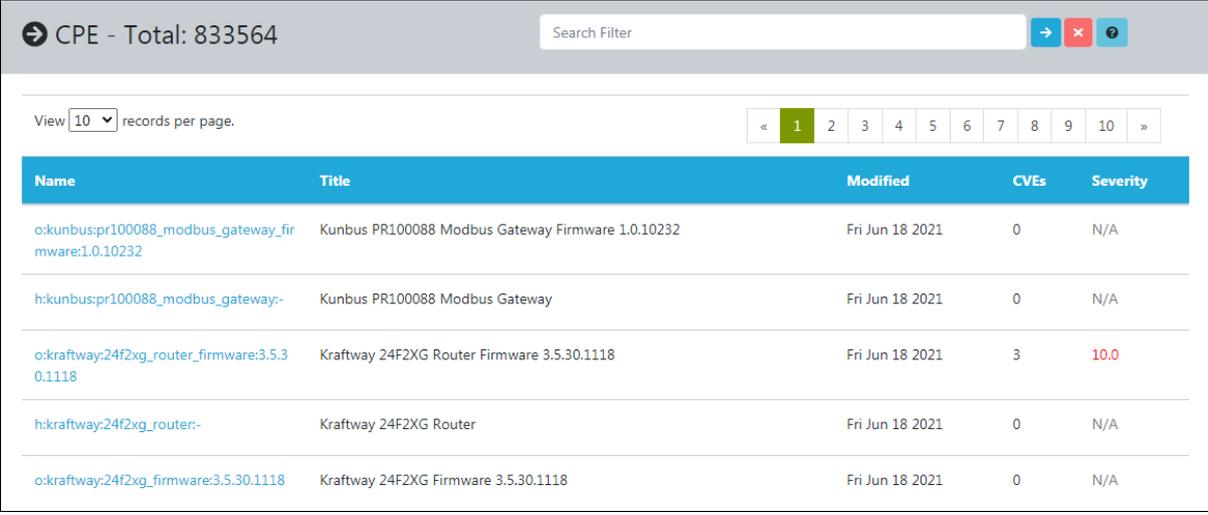
In 1999, The MITRE Corporation addressed this issue by founding the CVE project. Each vulnerability was allocated a special identifier that consists a year and number. The NVD (National Vulnerability Database) looks up MITRE's CVE database and provides the solution for vulnerability, its severity level, products affected and its impact. Nemasis refers 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 following filter tags:

- name
- 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 softwares 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 standard, the unique combination helps identify vulnerabilities quickly across a product or platform.



Name	Title	Modified	CVEs	Severity
o:kunbus:pr100088_modbus_gateway_firmware:1.0.10232	Kunbus PR100088 Modbus Gateway Firmware 1.0.10232	Fri Jun 18 2021	0	N/A
hkunbus:pr100088_modbus_gateway:-	Kunbus PR100088 Modbus Gateway	Fri Jun 18 2021	0	N/A
okraftway:24f2xg_router_firmware:3.5.30.1118	Kraftway 24F2XG Router Firmware 3.5.30.1118	Fri Jun 18 2021	3	10.0
hkraftway:24f2xg_router:-	Kraftway 24F2XG Router	Fri Jun 18 2021	0	N/A
okraftway:24f2xg_firmware:3.5.30.1118	Kraftway 24F2XG Firmware 3.5.30.1118	Fri Jun 18 2021	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 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 → ✕ ?

View records per page. « 1 2 3 4 5 6 7 8 9 10 »

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

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 following filter tags:

- name
- class
- cves
- severity

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

Configurations

The Configurations module consists following submodules:

- **Targets**
- **Port Lists**
- **Credentials**
- **Alerts**
- **Scan Configs**
- **Schedules**
- **Scanners**
- **False Positives**

Targets

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

[Add Target / Group](#)

Target / Group  

View records per page. < 1 2 3 4 5 6 7 8 9 10 >

Name	IP	Port List	Credentials	Actions
Sample Target 2	1	nemasis Default		   
Sample Target	1	nemasis Default		   

Add a Target

To add a Target,

1. Go to **Configurations > Target**.
2. Click **Add Target / Group**.
Add Target form appears.

Add Target

Name*:

Comment:

Host ? MANUAL

Exclude Host ? MANUAL

Reverse Lookup Only NO

Reverse Lookup Unify NO

Port List

Alive Test

Credentials for authenticated checks

SSH

SMB

ESXi

SNMP

3. Enter a name for the Target.
4. Enter a descriptive comment for the Target.

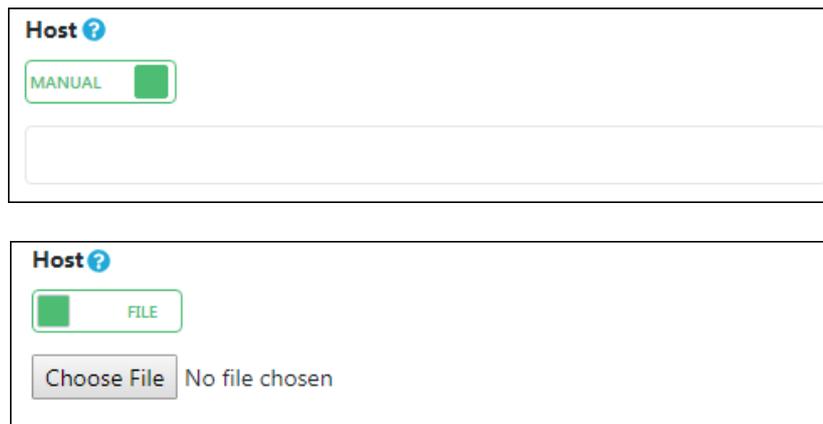
Host

Enter the IP address or import a list of IP addresses in this box. You can enter the IP address in the box with 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 list of IP addresses, click the **Host** toggle. The toggle will change from **MANUAL** to **FILE**.



The image shows two screenshots of the 'Host' configuration interface. The top screenshot shows the 'Host' toggle set to 'MANUAL' with a green square indicator. Below it is a text input field. The bottom screenshot shows the 'Host' toggle set to 'FILE' with a green square indicator. Below the toggle is a 'Choose File' button and the text 'No file chosen'.

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

5. Enter the details in Host box as per preferred method.

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 scan, click the **Exclude Host** toggle. The toggle will change from **MANUAL** to **FILE**.



The image shows two screenshots of the 'Exclude Host' configuration interface. The top screenshot shows the 'Exclude Host' toggle set to 'MANUAL' with a green square indicator. Below it is a text input field. The bottom screenshot shows the 'Exclude Host' toggle set to 'FILE' with a green square indicator. Below the toggle is a 'Choose File' button and the text 'No file chosen'.

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

6. Enter the details in Exclude Host box as per preferred method.

Reverse Lookup Only

Nemasis 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**.



7. Enable/Disable the Reverse Lookup Only toggle as per your preference.

Reverse Lookup Unify

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



Port List

Click the drop-down 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 drop-down:

- 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 scan if the system is a UNIX or Linux system.

SMB Credential

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

Credentials for authenticated checks

SSH **SMB**

-- --

22

Check SMB-SSH

After selecting the credentials for authenticated scan, if you wish to check the credentials click **Check SMB-SSH**. It will enable the user to check the login status of added hosts using defined credentials (connected or not).

Credentials for authenticated checks

SSH **SMB**

-- newcred

22

View SMB-SSH

Click **View SMB-SSH**, it will display the list of hosts along with the login status.

Login Status		
User	IP	Status
PT-50	192.168.0.0	NOT CONNECTED
PT-50	192.168.0.39	CONNECTED

Close

NOTE

This feature will work on all Chromium-based browsers, other browsers require SSL certificate.

ESXi Credential

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

SNMP Credential

Select this credential to log into the target system for 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 boxes, click **Add Target**. The new Target gets 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
-  View Asset Tag for 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,

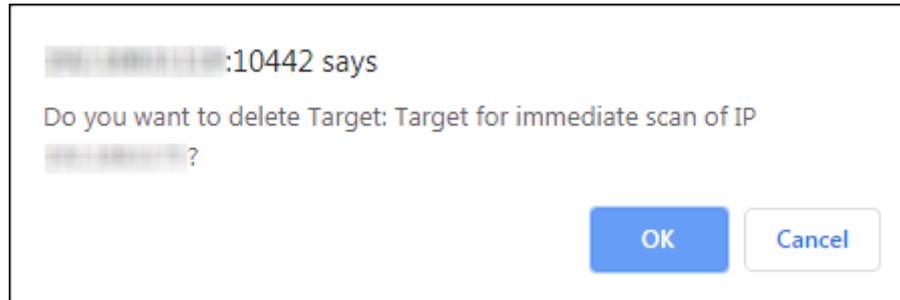
1. Go to **Scan > Task**.
Current Tasks list appears.
2. Find the Task to which the specific Target is assigned and then in the Actions column, click  (Edit Task).
Edit Task window appears.
3. Click the **Target and Alerts** tab.
4. Click the **Scan Targets** drop-down and select a different Target.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

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

Delete a Target

To delete a Target,

1. Go to **Configurations > Target**.
2. In the Actions column, click .
A confirmation prompt appears.



3. Click **OK**.
The Target gets deleted.

Clone a Target

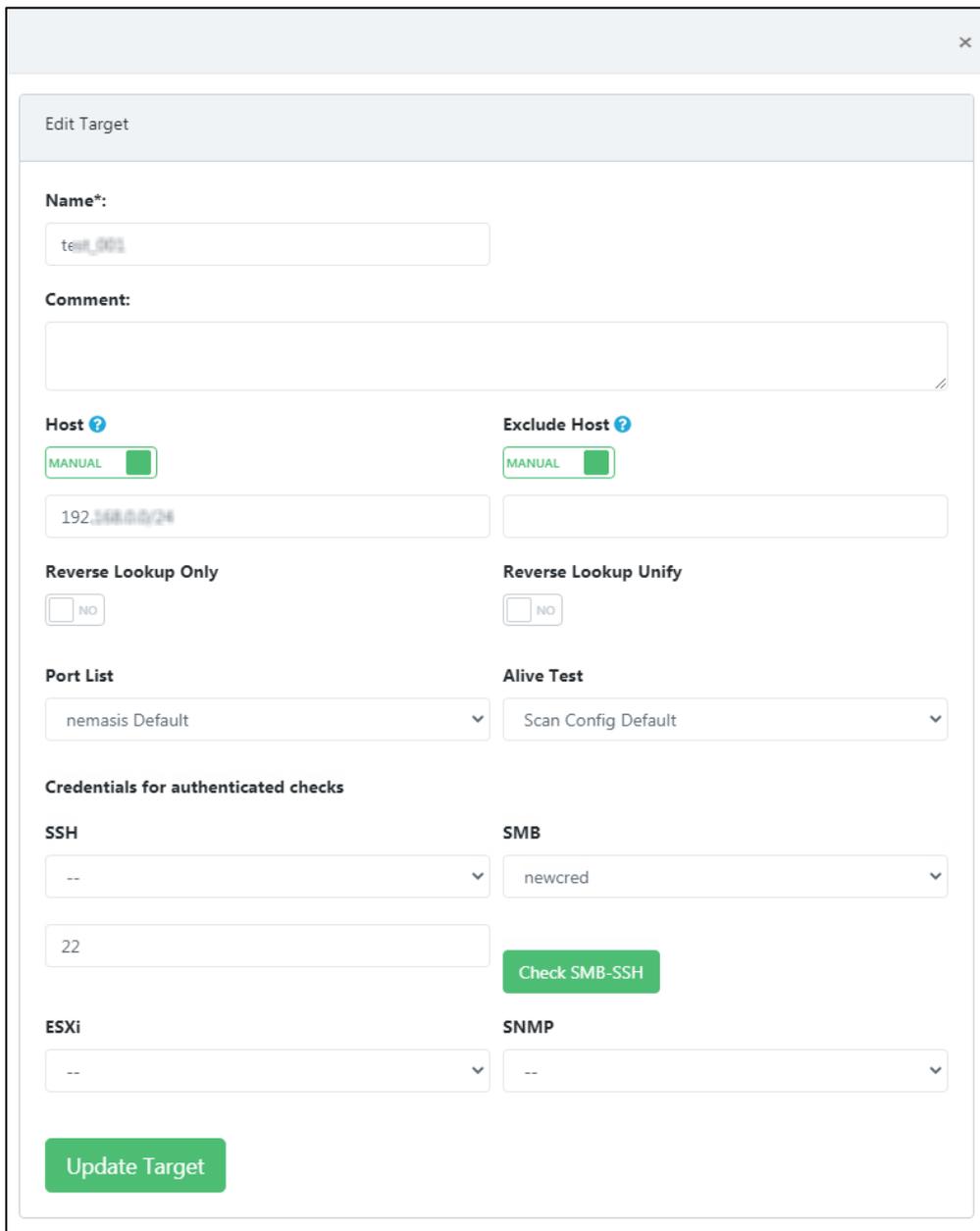
To clone a Target,

- Go to **Configurations > Target**.
- In the Actions column, click .
The Target gets cloned.

Edit a Target

To edit a Target,

1. Go to **Configurations > Target**.
2. In the Actions column, click . Edit Target window appears.



The screenshot shows the 'Edit Target' window with the following fields and options:

- Name*:** Input field containing 'test_001'.
- Comment:** Text area.
- Host ?**: Input field containing '192.168.0.24'. Below it is a 'MANUAL' toggle switch (checked).
- Exclude Host ?**: Input field (empty). Below it is a 'MANUAL' toggle switch (checked).
- Reverse Lookup Only**: Radio button 'NO' (unchecked).
- Reverse Lookup Unify**: Radio button 'NO' (unchecked).
- Port List**: Dropdown menu showing 'nemasis Default'.
- Alive Test**: Dropdown menu showing 'Scan Config Default'.
- Credentials for authenticated checks**:
 - SSH**: Dropdown menu showing '--'. Below it is an input field containing '22'.
 - SMB**: Dropdown menu showing 'newcred'. Below it is a green 'Check SMB-SSH' button.
 - ESXi**: Dropdown menu showing '--'.
 - SNMP**: Dropdown menu showing '--'.
- Update Target**: Green button at the bottom left.

3. Make the necessary changes and then click **Update Target**. The Target gets updated.

Port Lists

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

Add Port List

☰ Port Lists 🖨️ 🗑️

View 10 records per page. < 1 >

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	✎️ 🔍 🗑️ 🟢

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 is equipped with defaults Port lists that contain specific TCP and UDP ports for scanning.

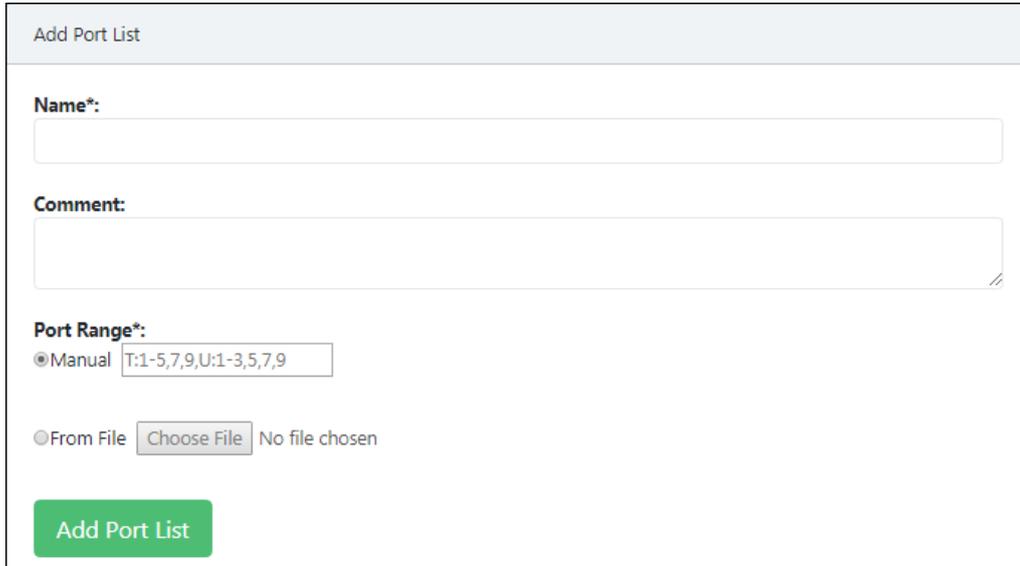
Normally, TCP ports get scanned fast. Operating systems that lack firewall features always respond to a TCP request and inform if the port is closed (TCP-RST) or open (TCP-ACK). The UDP ports behave in a different manner. The operating system replies consistently only if the port is closed (ICMP-Port-Unreachable). 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, 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.

Add a Port List

To add a Port List,

1. Go to **Configurations > Port List**.
2. Click **Add Port List**.
Add Port List window appears.



3. Enter a name for the Port List.
4. 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 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

5. Enter the Port Range as per preferred method.

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

6. Click **Add Port List**.
The Port List gets 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
-  View Asset Tag for Portlist

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,

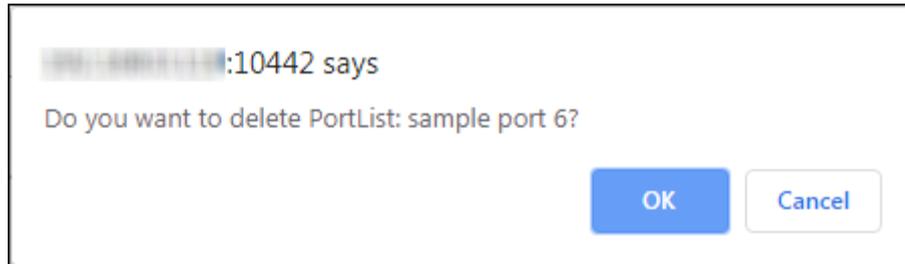
1. Go to **Configurations > Target**.
Targets list appears.
2. Find the Target to which the specific Port List is assigned and then in the Actions column, click  (Edit Target).
Edit Target window appears.
3. Click the **Port List** drop-down and select a different Port List.
4. Click **Update Target**.

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

Delete a Port List

To delete a Port List,

1. Go to **Configurations > Port List**.
2. In the Actions column, click .
A confirmation prompt appears.



3. Click **OK**. The Port List gets deleted.

Clone a Port List

To clone a Port List,

1. Go to **Configurations > Port List**.
2. In the Actions column, click .
The Port List gets cloned.

Edit a Port List

To edit a Port List,

1. Go to **Configurations > Port List**.
2. In the Actions column, click .
Edit Port List window appears.

Edit Port List

Name :

Comment :

Port Range :

TCP ▼ Add Port Range

Start	End	Protocol	Action
1	1	tcp	
3	3	udp	

Update Port List

3. Modify the port range by clicking TCP/UDP drop-down and then click **Add Port Range**.
4. After making the necessary changes, click **Update Port List**.
The Port List gets updated.

Credentials

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

[Add Credential](#)

Credentials

View records per page. « 1 2 3 »

Name	Type	Allow insecure use	Login	Actions
Sample Credential 2	username + password (up)	No	Sample2	   
Sample Credential	username + password (up)	No	Sample	   

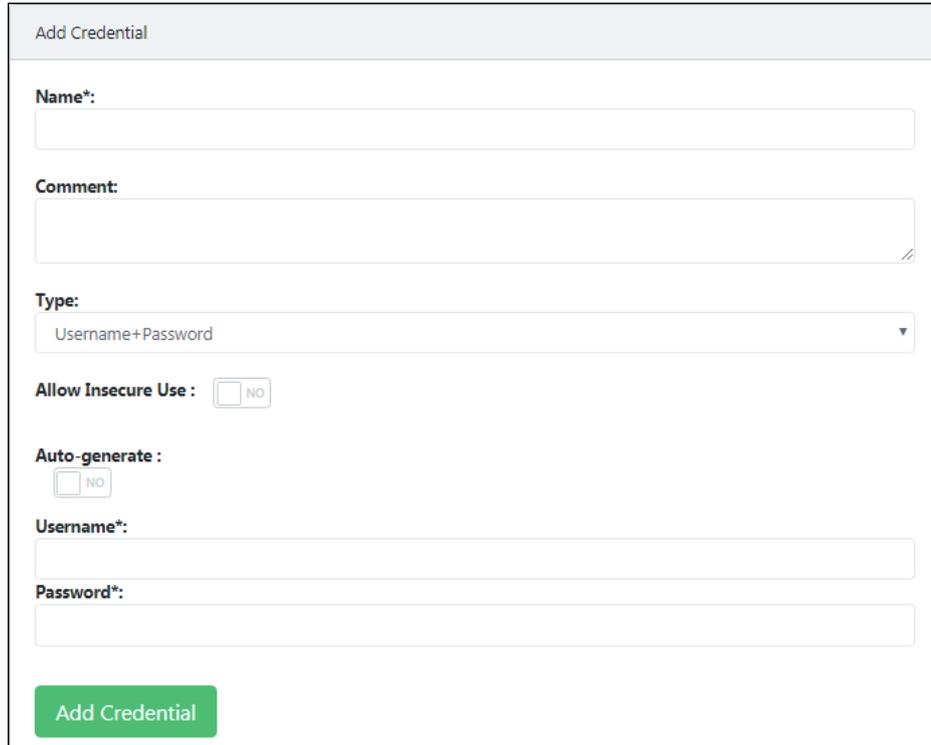
With the login credentials, the scan plugins get access to the target system and carry out local security checks. An authenticated scan provides you with all remotely detectable and exploitable vulnerabilities, whereas an unauthenticated scan will display only the remotely detectable vulnerabilities. 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 will use similar protocols and techniques as of a hacker, to gain access of a target system and carry out test 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.

Add a Credential

To add a Credential,

1. Go to **Configurations > Credentials**.
2. Click **Add Credential**.
Add Credential window appears.



The screenshot shows a web form titled "Add Credential". It contains the following fields and controls:

- Name*:** A text input field.
- Comment:** A text area for a descriptive comment.
- Type:** A dropdown menu with "Username+Password" selected.
- Allow Insecure Use :** A toggle switch currently set to "NO".
- Auto-generate :** A toggle switch currently set to "NO".
- Username*:** A text input field.
- Password*:** A text input field.
- Add Credential** button: A green button at the bottom left.

3. Enter a name for the Credential.
4. Enter a descriptive comment for the Credential.
5. Click the **Type** drop-down and select a preferred authentication.

Allow insecure use

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

6. Select preferred method for **Allow insecure use** option.

Autogenerate Credentials

The NEMASIS will autogenerate a password for the Credential. By default this option is set to **NO**. Click the toggle to change it to **YES**.

7. Select preferred method for **Autogenerate Credentials** option.

For Username+Password type authentication

Type:
Username+Password

Allow Insecure Use : NO

Auto-generate :
 NO

Username*:

Password*:

1. Enter the target system's credentials.
2. After filling all the boxes, click **Add Credential**.
The Credential gets added to the Credentials list.

For Username+SSH Key type authentication

Type:
Username+SSH Key

Allow Insecure Use : NO

Auto-generate :
 NO

Username*:

Password*:

Private Key*:
 No file chosen

1. Enter the target system's credentials.
2. The login process can be completed via SSH. Click **Choose File** and then select the private key from the destination path.
3. After filling all the boxes, click **Add Credential**.
The Credential gets added to the Credentials list.

For SNMP type authentication

Type:

Allow Insecure Use : NO

SNMP Community*:

Username*:

Password*:

Privacy Password :

Auth Algorithm*:
 MD5 SHA1

Privacy Algorithm :
 MD5 DES None

1. Enter the protocols used for the SNMP community.
2. Enter the SNMP credentials.
3. Enter the Privacy Password to encrypt the communication in the SNMP system.
4. Select the preferred Authentication Algorithm.
5. Select the preferred Privacy Algorithm.
6. After filling all the boxes, click **Add Credential**.
The Credential gets 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
-  View Asset Tag for Credentials

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,

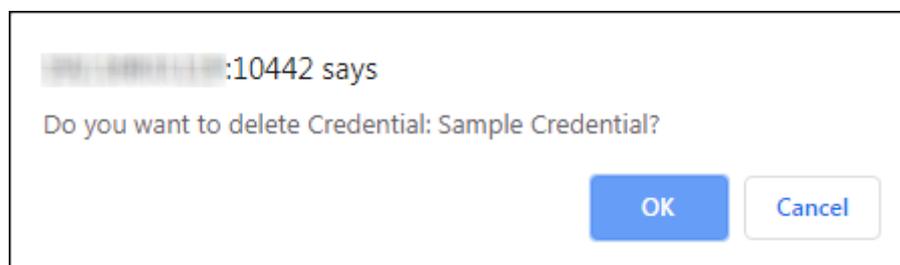
1. Go to **Configurations > Target**.
Targets list appears.
2. Find the Target to which the specific Credential is assigned and then in the Actions column, click  (Edit Target).
Edit Target window appears.
3. Click the appropriate **Credential** drop-down and select a different Credential.
4. Click **Update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

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

Delete a Credential

To delete a Credential,

1. Go to **Configurations > Credential**.
2. In the Actions column, click .
A confirmation prompt appears.



3. Click **OK**.
The Credential gets deleted.

Clone a Credential

To clone a Credential,

1. Go to **Configurations >Credential**.
2. In the Actions column, click .
The Credential gets cloned.

Edit a Credential

To edit a Credential,

1. Go to **Configurations >Credential**.
2. In the Actions column, click .
Edit Credential window appears.

Edit Credential

Name :

Comment :

Type :

Allow Insecure Use: NO

Username :

Password :

3. Make the necessary changes and then click **Update Credential**.
The Credential gets 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 scenario, you can configure the Nemasis 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 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.

Add Alert

Alerts
🖨️ | 🗕

View records per page.
« 1 2 3 4 5 6 7 8 9 10 »

Name	Event	Condition	Method	Active	Actions
Sample Alert 3	Task run status changed to stop requested	Always	Email to user@domain.com	Yes	
Sample Alert 2	Task run status changed to stopped	Always	Email to user@domain.com	Yes	
Sample Alert	Task run status changed to done	Always	Email to user@domain.com	Yes	

Add an Alert

To add an Alert,

1. Go to **Configurations > Alerts**.
2. Click **Add Alert**.

Add Alert window appears.

Add Alert

Name*:

Comment:

Event:

Task run status changed to New

Conditions :

Always Severity at least Severity Level

Method :

To Address* : **From Address* :**

Subject :

Content :

Simple Notice

Include Report

Task '\$n': \$e

Attach Report

Task '\$n': \$e

Active

3. Enter a name for the Alert.
4. Enter a descriptive comment for the Alert.

Event

You can specify when you want to receive an Alert. Following options are available:

- **Task run status changed to**

Click the drop-down 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 database or get updated.

Conditions

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

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

Method

Click the drop-down and select a 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.

Following methods can be used to receive an event alert.

- A. Email**
- B. SCP**
- C. Send to host (e.g. Splunk)**
- D. Send Event**
- E. SMB**
- F. Start Another Task**

1. Email

To Address

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

From Address

Enter the email address for the Nemasis 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 box.

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 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 TXT file attachment containing all the details.

2. SCP

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

Method :
SCP

Credentials : Sample Credential ▾ **Host*:**

Known Host :

Path*: **Report :** Anonymous XML ▾

Active

Add Alert

Enter the following variables within the filename:

- \$\$: \$
- \$n: Task Name

Credentials

Click the drop-down 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 box.

Path

Enter the destination path where you want to the report to be stored.

For example, /Users/QA/Desktop

Report

Click the drop-down and select the appropriate format for Report.

3. Send to Host (e.g. Splunk)

You can send the report via TCP to a Host/Port combination.

Method :
Send to host (e.g. Splunk) ▼

Send to Host*:
 on port

Report :
Anonymous XML ▼

Active

Add Alert

Send to Host

Enter the IP address of the system on which you want to receive the report.

On Port

Enter the appropriate Splunk port number.

Report

Click the drop-down and select the appropriate format for Report.

4. Send Event

You can send the Nemasis scanner events via TCP to a Host/Port combination.

Method :

Send to Host*:
 on port

Active

Send to Host

Enter the IP address of the system on which you want to receive the report.

On Port

Enter the appropriate port number.

5. SMB

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

Method :
SMB ▼

Credential: Sample Credential ▼ **Share Path*:**

File Path*: **Report** Anonymous XML ▼

Active

Add Alert

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 drop-down 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 drop-down and select the appropriate format for the Report.

6. Start Another Task

Selecting this method lets you run another task.

Method :

Start Another Task ▼

Task :

Sample Task ▼

Active

Add Alert

Task

Click the drop-down and select the task you want Nemasis to run after finishing current task.

After filling all the boxes, click **Add Alert**. The new Alert gets 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
-  View Asset Tag for 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,

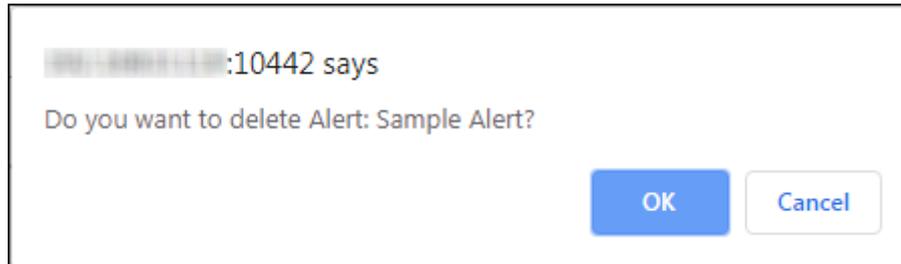
1. Go to **Scan > Task**.
Current Tasks list appears.
2. Find the Task to which the specific Alert is assigned and then in the Actions column, click  (Edit Task).
3. Click **Targets and Alerts** tab.
4. Click the **Alerts** drop-down and select a different Alert.
5. Click **Update Task**.

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

Delete an Alert

To delete an Alert,

1. Go to **Configurations > Alerts**.
2. In the Actions column, click .
A confirmation prompt appears.



3. Click **OK**.
The Alert gets deleted.

Clone an Alert

To clone an Alert,

1. Go to **Configurations > Alerts**.
2. In the Actions column, click .
The Alert gets cloned.

Edit an Alert

To edit an Alert,

1. Go to **Configurations > Alerts**.
2. In the Actions column, click .
Edit Alert window appears.

Edit Alert

Name*:

Comment:

Event:
 Task run status changed to New

Conditions :
 Always Severity at least Severity Level

Method :

✕

To Address* : **From Address* :**

Subject :

Content :
 Simple Notice
 Include Report

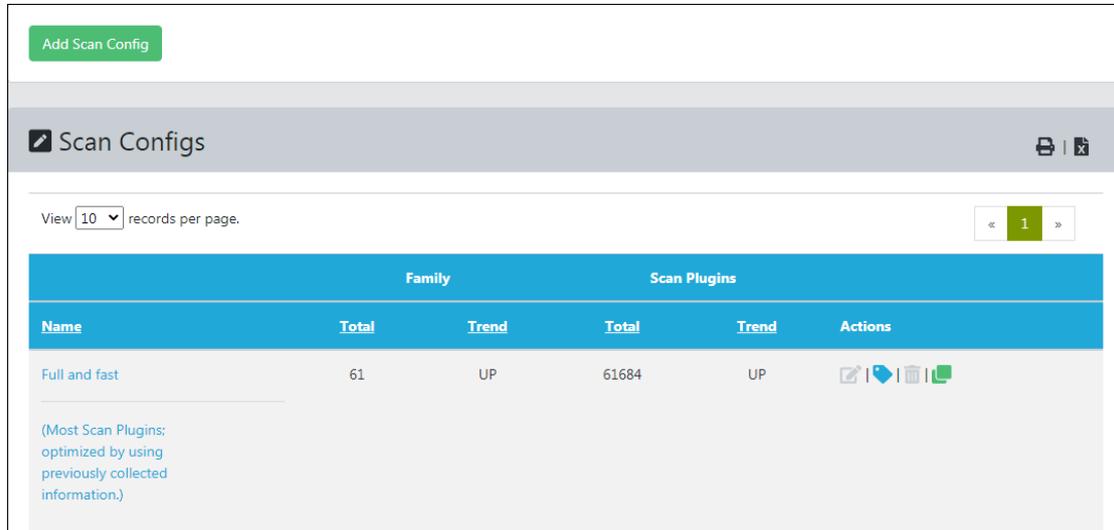
 Attach Report

Active

3. Make the necessary changes and then click **Update Alert**. The Alert gets updated.

Scan Configs

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



The screenshot shows a web interface for managing scan configurations. At the top left is a green button labeled 'Add Scan Config'. Below it is a header bar with a checkmark icon and the text 'Scan Configs', along with print and refresh icons. A pagination control shows 'View 10 records per page.' and a page number '1'. The main content is a table with the following structure:

Name	Family		Scan Plugins		Actions
	Total	Trend	Total	Trend	
Full and fast	61	UP	61684	UP	   

Below the table, there is a note: '(Most Scan Plugins: optimized by using previously collected information.)'

The Nemasis 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. This scan configuration is most preferred as it consists of Scan Plugins suitable for all environments.
- **Full and Fast Ultimate**
This configuration expands the first configuration with Scan Plugins that may cause a system shutdown or disrupt running services.
- **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.

- 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.
- Empty**
 If you do not want any scan configuration for the task, select this configuration.
- Discovery**
 This configuration uses Scan Plugins that provides the Target's most accurate information. This configuration does not detect any vulnerability.
- 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 name, you can view its current and default value.

Scanner Preferences : Full and fast		
Scanner Preferences (18)	Plugin Families (62)	Plugin Preferences (5259)
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 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.

Add a Scan Config

To add a Scan Config,

1. Go to **Configurations > Scan Config**.
2. Click **Add Scan Config**.
Add Scan Config window appears.

Add Scan Config

Name :

Comment :

Base :
 Empty, static and fast Full and fast

Add Scan Config

3. Enter a name for the Scan Configuration.
4. Enter a descriptive comment for the Scan Configuration.
5. Select a preferred scan base from following options:
 - **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 CISCO family.
 - **Full and fast**
Select this scan configuration to scan the target by using all scan plugin families.
6. Click **Add Scan Config**.
The Scan Configuration gets 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
-  View Asset Tag for 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 window appears.
3. Click the **Scanner and Config** tab.
4. Click the **Scan Config** drop-down and select a different Scan Config.
5. Click **Update Task**.

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

Delete a Scan Config

To delete a Scan Config,

1. Go to **Configurations > Scan Config**.
2. In the Actions column, click .
A confirmation prompt appears.



3. Click **OK**.
The Scan configuration gets deleted.

Clone a Scan Config

To clone a Scan Config,

1. Go to **Configurations > Scan Config**.
2. In Actions column, click .
The Scan Config gets cloned.

Edit a Scan Config

To edit a Scan Config,

1. Go to **Configurations > Scan Config**.
2. In the Actions column, click .
Edit Scan Config window appears.

Edit Scan Config

Name :

Comment :

Edit Scan Plugin Families 

Edit Scanner Preferences 

Scan Plugin Preferences 

3. Make the necessary changes and then click **Update Scan Config**.
The Scan Config gets updated.

Schedules

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

[Add Schedule](#)

Schedules 🖨️ | 📄

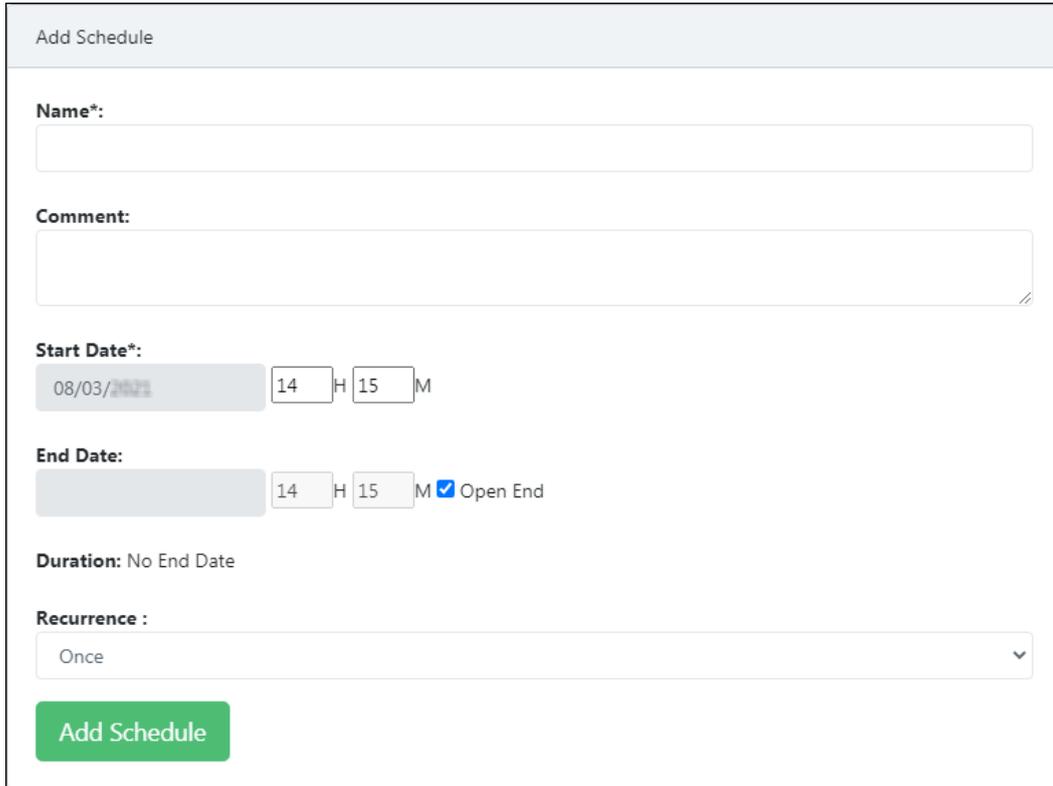
View records per page. « 1 2 »

Name	First Run	Next Run	Recurrence	Duration	Actions
Sample Schedule 2	Jan 21 2021 03:00 PM	-	Once	24 Hours	   
Sample Schedule 1	Jan 21 2021 02:59 PM	-	Once	No End Date	   

Add a Schedule

To add a Schedule,

1. Go to **Configurations >Schedule**.
2. Click **Add Schedule**.
Add Schedule window appears.



The screenshot shows the 'Add Schedule' form with the following fields and options:

- Name*:** A text input field.
- Comment:** A text area for adding a descriptive comment.
- Start Date*:** A date and time selector showing '08/03/2021' and '14 H 15 M'.
- End Date:** A date and time selector showing '14 H 15 M' and a checked checkbox for 'Open End'.
- Duration:** A label indicating 'No End Date'.
- Recurrence :** A dropdown menu currently set to 'Once'.
- Add Schedule:** A green button at the bottom of the form.

3. Enter a name for the Schedule.
4. Enter a descriptive comment for the Schedule.
5. Select a Start Date and time for the Schedule to run.
6. Select an End Date and time for the Schedule to end.
If you want the Task to run at regular intervals, select the checkbox **Open End**.
After selecting this checkbox, **End Date** box gets disabled.

Open End

Select this checkbox if you want the Task to run at regular intervals. After its selection, the **End Date** box gets disabled.

Duration

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

Recurrence

Click the drop-down and select the option on which you want the Schedule to recur.

Following options are available.

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

7. Click **Add Schedule**. The new Schedule gets 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,

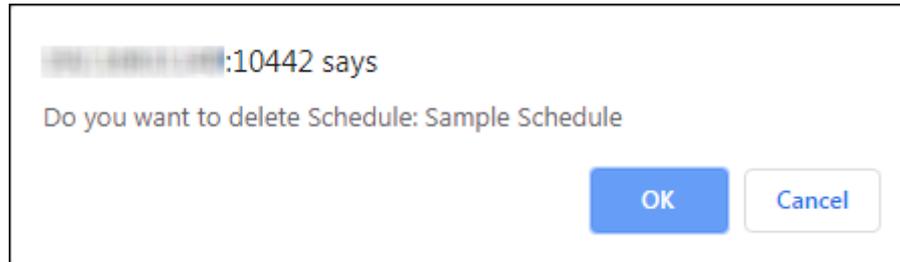
1. Go to **Scan > Task**.
Current Tasks list appears.
2. Find the Task to which the specific Schedule is assigned and then in the Actions column, click  (Edit Task).
Edit Task window appears.
3. Click the **Target and Alerts** tab.
4. Click the **Schedule** drop-down and select a different Schedule.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

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

Delete a Schedule

To delete a Schedule,

1. Go to **Configurations > Schedule**.
2. In the Actions column, click .
A confirmation prompt appears.



3. Click **OK**.
The Schedule gets deleted.

Clone a Schedule

To clone a Schedule,

1. Go to **Configurations > Schedule**.
2. In the Actions column, click .
The Schedule gets cloned.

Edit a Schedule

To edit a Schedule,

1. Go to **Configurations > Schedule**.
2. In the Actions column, click .
Edit Schedule window appears.

Edit Schedule

Name*:

Comment:

Time Zone:

Start Date*:
 H M

End Date:
 H M Open End

Duration: 24 Hours

Recurrence :

3. Make the necessary changes and then click **Update Schedule**.
The Schedule gets updated.

Scanners

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

The Scanners submodule lets you add a scanner hosted on another system.

[Add Scanner](#)

Scanners 🖨️ | 🗕

View records per page. « 1 »

Name	Host	Port	Type	Credential	Actions
nemasis Default		0	NEMASIS Scanner		✎ 📄 🗑️ 📄
CVE		0	CVE Scanner		✎ 📄 🗑️ 📄

Add a Scanner

To add a Scanner,

1. Go to **Configurations > Scanner**.
2. Click **Add Scanner**.
Add Scanner window appears.

Add Scanner

Name*:

Comment:

Host*: **Port*:**

Scanner: **Credential*:**

CA Certificate :
 No file chosen

3. Enter a name for the Scanner.
4. Enter a descriptive comment for the Scanner.
5. In the Host box, enter the IP address of the system in which Scanner is installed.
6. In the Port box, enter the Port Number.
7. Click the Scanner drop-down and select the preferred Scanner.
 - **NSP Scanner**
The Nemasis Scanner Protocol lets you control secondary vulnerability scanners. These scanners must either offer the protocol NSP on their own. The Nemasis UI lets you configure NSP scanners via section Configuration/Scanner.
 - **NMP Scanner**
Nemasis Manage Protocol lets you control secondary vulnerability scanner running with NMP protocol.
8. Click the Credential drop-down and select the appropriate credentials.
9. Add CA Certificate by clicking **Choose File** and select the file from the system.
10. Click **Add Scanner**.
The Scanner gets added to the Scanners list.

**NOTE**

The Nemasis Default and CVE are default scanning engines and cannot be deleted, edited or cloned.

Actions

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

-  Delete Scanner
-  Edit Scanner
-  Clone Scanner
-  View Asset Tag for Scanner

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

-  Delete Scanner (in use)

In order to delete such a Scanner,

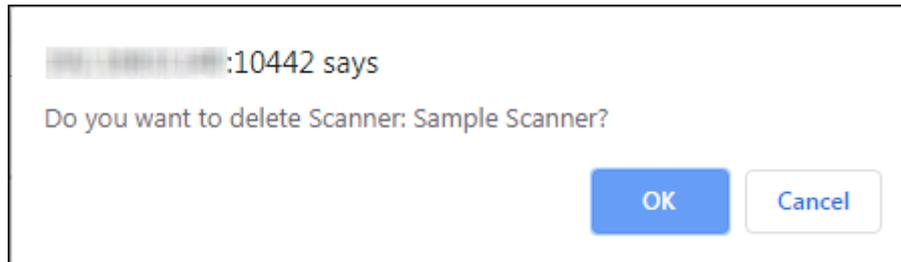
1. Go to **Scan > Task**.
Current Tasks list appears.
2. Find the Target to which the specific Scanner is assigned and then in the Actions column, click  (Edit Task).
Edit Task window appears.
3. Click the **Scanner and Config** tab.
4. Click the **Scanner** drop-down and select a different Scanner.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

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

Delete a Scanner

To delete a Scanner,

1. Go to **Configurations** > **Scanner**.
2. In the Actions column, click .
A confirmation prompt appears.



3. Click **OK**.
The Scanner gets deleted.

Clone a Scanner

To clone a Scanner,

1. Go to **Configurations** > **Scanner**.
2. In the Actions column, click .
The Scanner gets cloned instantly.

Edit a Scanner

To edit a Scanner,

1. Go to **Configurations > Scanner**.
2. In the Actions column, click .
Edit Scanner window appears.

Edit Scanner

Name*:

Comment:

Host*: **Port*:**

Scanner: **Credential*:**

CA Certificate :
 No file chosen

3. Make the necessary changes and then click **Update Scanner**.
The Scanner gets updated.

False Positives

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.

Add False Positive

False Positives
🖨️ 📄

View records per page.
« 1 2 3 »

Scan Plugin	Comments	Task	Host IPs	Active	Actions
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) Plugin ID: 1.3.6.1.4.1.25623.1.0.902269	This is a accepted risk since the compensating controls (Firewall Policies and EPS Policies are in a continuous monitoring mode whereby the any incoming traffic is analyzed and if detected Malicious corrective actions like blocking alerts and logging is performed. These activities are constantly monitored by the IT Security team for further judgmental analysis.)	All Tasks	192.168.0.48	✔️	📄 🗑️
Cisco ACE Application Control Engine Detection Plugin ID: 1.3.6.1.4.1.25623.1.0.106257	plain comment	All Tasks	All Hosts	✔️	📄 🗑️

Vulnerability scanners frequently find evidence that point 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 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 situation, he/she can make sure that this finding is not displayed next time.

Add a False Positive

To add a False Positive,

1. Go to **Configurations > False Positive**.
2. Click **Add False Positive**.
Add False Positive window appears.

Add False Positive

Select Scan Plugin*:

Severity*:

False Positive ▼

Active*: Yes Active for Days No

Task :

All Tasks ▼

Host IPs :

Leave blank for all Host IPs

Comment*:

Add False Positive

3. In the **Select Scan Plugin** box, enter your finding and select the appropriate finding from suggestions.
4. Click the **Severity** drop-down and modify the severity of a finding.
The drop-down consists of 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.

5. Select the **Active** option. It has following options:
 - **Yes** – This will enable the False positive option.
 - **Active for _ Days** – This will enable the False positive option for the specific number of days.
 - **No** – This will create the False positive but the option will be disabled.
6. Select the task for which you want to enable the False positive option.
7. Enter the particular IPs for which you want to enable this option.
8. Enter a descriptive comment for the False Positive.
9. Click **Add False Positive**.
The False Positive gets added to the False Positives list.

Actions

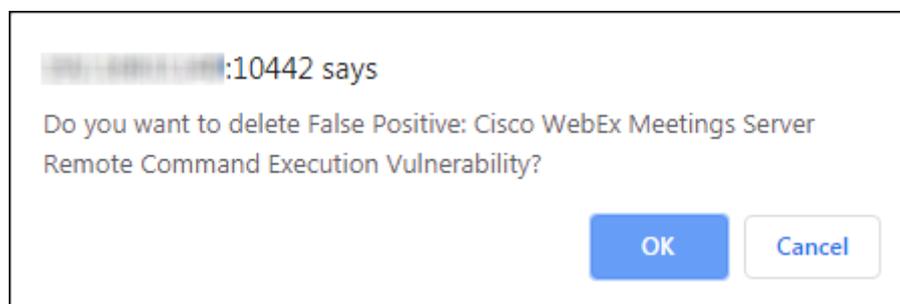
Clicking icons in the Actions column lets you take actions regarding a False Positive.

-  Delete False Positive
-  View Asset Tag for False Positive

Delete a False Positive

To delete a False Positive,

1. Go to **Configurations > False Positive**.
2. In the Actions column, click .
A confirmation prompt appears.



3. Click **OK**.
The False Positive gets deleted.

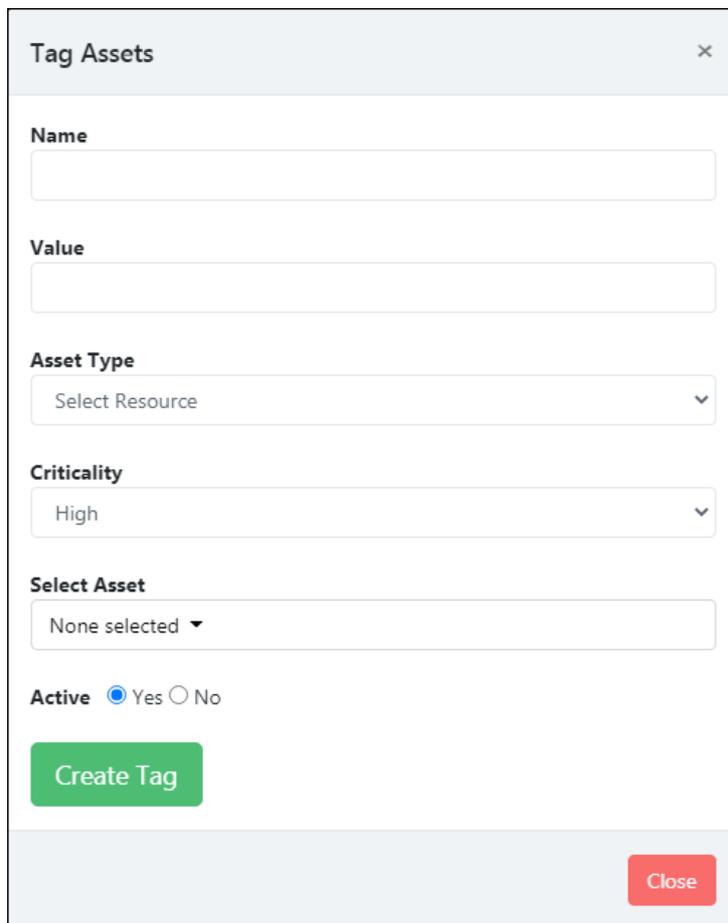
Asset Tagging

Asset tagging is a process of affixing a tag to identify and track data or events of that particular asset. It is primarily composed of Key-Value pair.

Add an Asset Tag

To add an Asset Tag,

1. Go to **Configurations > Asset Tagging**.
2. Click **Add Asset Tag**.
Tag Assets window appears.



3. Enter the **Name** and **Value** for the tag.
4. Select resource type for which the tag can be assigned in the drop-down list **Asset Type**.
5. Select the **Criticality** drop-down and modify it.
The drop-down consists of following options:
 - **High** – The asset will be considered as High criticality.
 - **Medium** – The asset will be considered as Medium criticality.
 - **Low** – The asset will be considered as Low criticality.
6. Select the Asset for tagging from the drop-down list.

7. Select **Active** option. It has following options:
 - **Yes** – This will enable the asset tag of particular asset.
 - **No** – This will disable the asset tag of particular asset.
8. Click **Create Tag**.
The asset will be added to the Asset Tagging list.

Actions

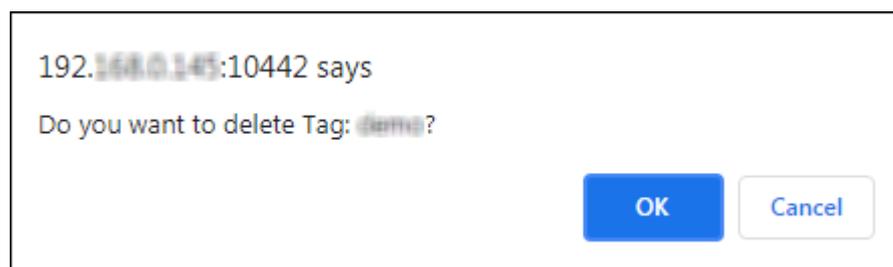
Clicking icons in the Actions column lets you take actions regarding an Asset tag.

-  Delete Asset tag
-  Edit Asset tag

Delete an Asset Tag

To delete an Asset Tag,

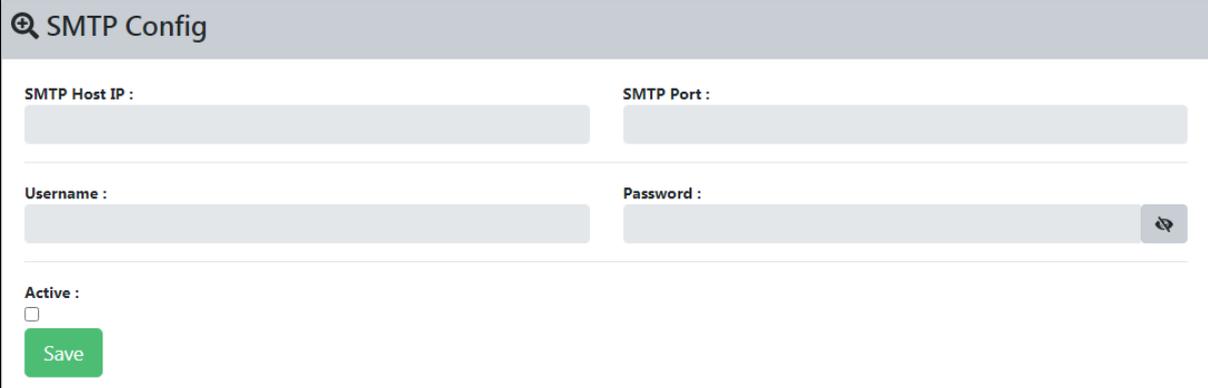
1. Go to **Configurations > Asset Tagging**.
2. In the **Actions** column, click .
A confirmation prompt appears.



3. Click **OK**.
The Asset Tag gets deleted.

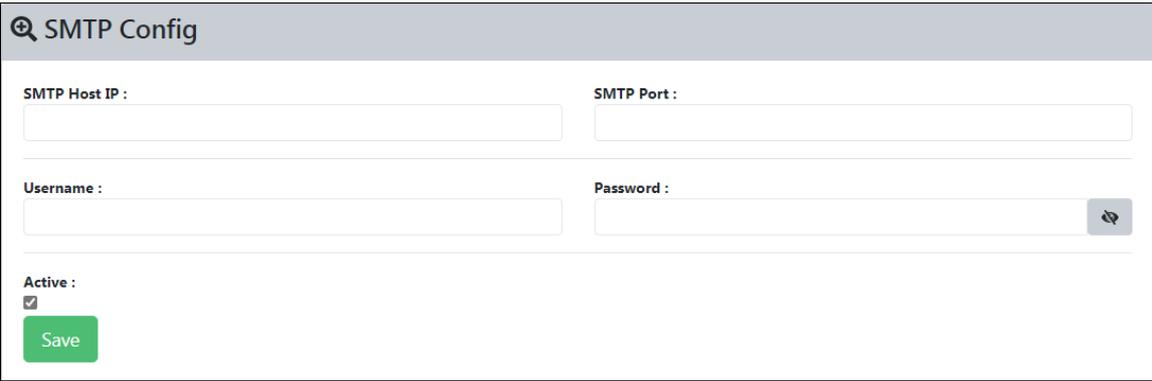
SMTP

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



The screenshot shows the 'SMTP Config' form. It has a header with a search icon and the text 'SMTP Config'. Below the header are four input fields: 'SMTP Host IP', 'SMTP Port', 'Username', and 'Password'. The 'Active' checkbox is unchecked. A green 'Save' button is at the bottom left.

Select the **Active** checkbox. This will enable all the boxes.



The screenshot shows the 'SMTP Config' form. It has a header with a search icon and the text 'SMTP Config'. Below the header are four input fields: 'SMTP Host IP', 'SMTP Port', 'Username', and 'Password'. The 'Active' checkbox is checked. A green 'Save' button is at the bottom left.

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 boxes.



- SMTP Password is visible



- SMTP Password is hidden

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

Administration

The Administration module lets you add new users, assign roles, define type of authentication, and add LDAP. The Administration contains following submodules:

- **Users**
- **Roles**
- **Secure LDAP**
- **Customize Header**
- **User Settings**

Users

The Users submodule lets you add users, set authentication and role for them.

[Add User](#)

 **Users**

View records per page. « 1 »

Name	Roles	Host Access	Interface Access	Auth. Type	Actions
Johnny	Admin	Allow all	Allow all	Local	  
Jon	Guest	Allow all	Allow all	Local	  
Jane	Info	Allow all	Allow all	Local	  
Adam	Monitor	Allow all	Allow all	Local	  
Eve	Observer	Allow all	Allow all	Local	  
Ana	User	Allow all	Allow all	Local	  

Add a User

To add a User,

1. Go to **Administration > Users**.
2. Click **Add User**.
Add User form appears.

Add User

Login Name*:

Comment :

Authentication :

Password

LDAP Authentication Only

Roles:

Admin ▼

Add User

3. Enter a name for the User.
4. Enter a descriptive comment for the User.
5. Select the appropriate Authentication for the User login.
If you are selecting the option **Password**, specify the password in the box next to it.
6. Click the Roles drop-down and select the appropriate role for the User.
The Roles and their accessible modules are mentioned below:
 - **Admin** – All modules
 - **Guest** – Dashboard, Security Info
 - **Info** – Dashboard, Security Info
 - **Monitor** – Dashboard
 - **Observer** – Dashboard, Scan, Assets, Task Results, Reports, Security Info, Configurations

- **User** – Dashboard, Scan, Assets, Task Results, Reports, Security Info, Configurations
7. Click **Add User**.
The new User gets added to the Users list.

 NOTE	An individual User will have access to only their activities. Admin is the superuser and has access to all users' activities.
--------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------

Actions

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

-  Delete User
-  Edit User
-  Clone User

Delete a User

To delete a User,

1. Go to **Administration > Users**.
2. In the Actions column, click .
A confirmation prompt appears.



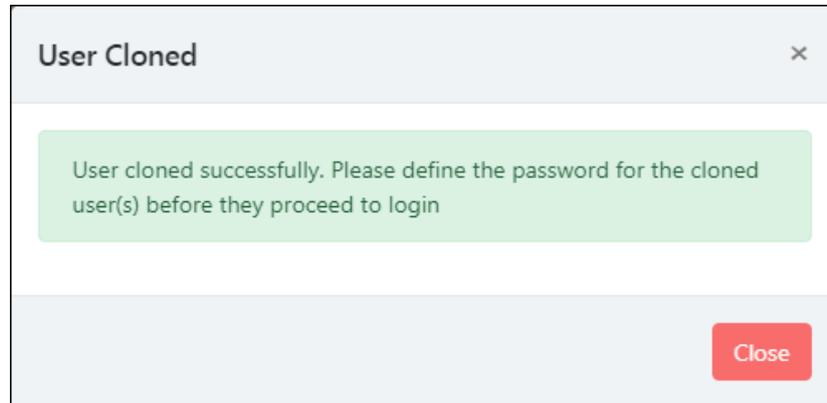
3. Click **OK**.
The User gets deleted.

 NOTE	A User won't get deleted if a scan task created by them is in progress.
----------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------

Clone a User

To clone a User,

1. Go to **Administration > Users**.
2. In the Actions column, click . A success message appears.

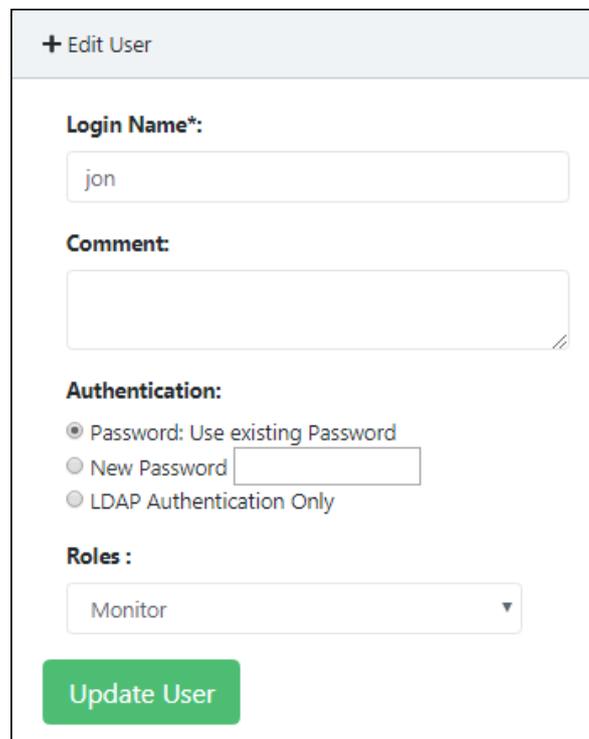


3. Close this message and then define the password for the Cloned User.

Edit a User

To edit a User's details,

1. Go to **Administration > Users**.
2. In the Actions column, click . Edit User window appears.



A form titled "+ Edit User" with the following fields and options:

- Login Name*:** Text input field containing "jon".
- Comment:** Text area field.
- Authentication:** Radio button options:
 - Password: Use existing Password
 - New Password
 - LDAP Authentication Only
- Roles :** Dropdown menu showing "Monitor".
- Update User** button.

3. Make the necessary changes and then click **Update User**. The User detail gets updated.

Roles

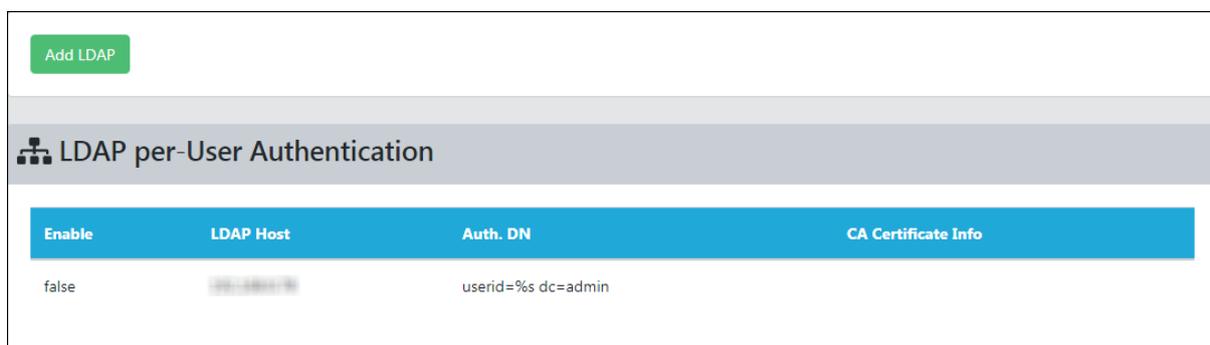
The Roles submodule displays the list of users and roles assigned to them.

Roles		
Name	Comment	Users
Admin	Administrator Full privileges	Johnny
Guest	Guest	Jon
Info	Information browser	Jane
Monitor	Performance monitor	Adam
Observer	Observer	Eve
Super Admin	Super administrator Full privileges with access to all users	admin
User	Standard user	Ana

Secure LDAP (LDAPS)

The Lightweight Directory Access Protocol (LDAP) is an industry standard application protocol for accessing and maintaining directory services across an organization. Nemasis uses a plain interface to add an LDAP. Normally the LDAP supporting systems search the LDAP tree for the matching object and after finding the object log in as the same (Search and Bind). The Nemasis utilizes a simple bind with a hard coded object path.

The Secure LDAP submodule displays added LDAPs and lets you add an LDAP.



The screenshot shows a web interface for LDAP configuration. At the top left is a green button labeled "Add LDAP". Below it is a header "LDAP per-User Authentication" with a tree icon. Underneath is a table with a blue header row and one data row.

Enable	LDAP Host	Auth. DN	CA Certificate Info
false	[REDACTED]	userid=%s dc=admin	

The DN (Distinguished Name) of an object can be defined in a distinctive manner. Thereby, the username is replaced by wildcard %s. Some examples for Auth. DN are mentioned below:

- cn=%s,ou=people,dc=domain,dc=de
- uid=%s,ou=people,dc=domain,dc=de
- %s@domain.de
- domain.de\%s

With correct attributes, the first two examples work for all LDAP servers. For an Active Directory, the third and fourth examples can be used.

Hereby the exact location of the user object is irrelevant.

The first example is unable to support users in different recursive depths of an LDAP tree or different sub trees. It is necessary that every user that logs into Nemasis must be in the same branch and level of an LDAP tree.

In second example,

uid = user is used as a filter

ou = people

dc = domain

dc = org

The above mentioned attributes are used as base objects to carry out a search and get the corresponding DN for authentication. As the **uid** attribute is important it should be typed first.

Add an LDAP

To add an LDAP,

1. Go to **Administration > Secure LDAP**.
2. Click **Add LDAP**.
LDAP per User authentication form appears.

LDAP per-User Authentication

Enable :

LDAP Host*:

Auth. DN* :

CA Certificate :
 No file chosen

3. Select the **Enable** checkbox.
4. In the LDAP Host box, enter the IP address of the LDAP Host server. The Nemasis will access the LDAP host via SSL/TLS.
5. In the Auth. DN box, enter the appropriate Distinguished Name.
6. Add a CA Certificate by clicking **Choose File** and select the CA certificate from the system. For verification of the LDAP Host, it is necessary that you upload its CA certificate to the Nemasis.
7. Click **Save**.
The LDAP configuration gets saved.

**NOTE**

Nemasis will refuse the LDAP authentication without the SSL/TLS. If the LDAP authentication fails, please check whether the LDAP Host entry matches the commonName of the certificate of the LDAP server. If the entries do not match, Nemasis will refuse the LDAP server use.

Customize Header

The Customize Header submodule lets you customize the report header appearing on each page.



H Custom Header

Select Image* :

Choose File No file chosen

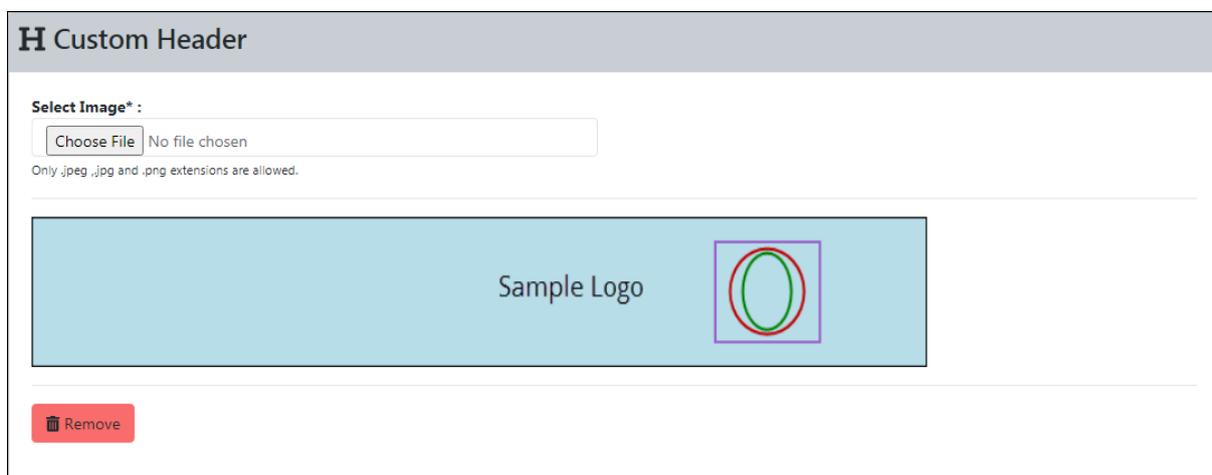
Only .jpeg, .jpg and .png extensions are allowed.

No Header Image Found

Add a Custom Header

To add a custom header,

1. Go to **Administration** > **Customize Header**.
2. Click **Choose File**.
File selection window appears.
3. Select the preferred file.

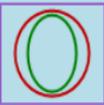


H Custom Header

Select Image* :

Choose File No file chosen

Only .jpeg, .jpg and .png extensions are allowed.

Sample Logo 

Remove

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



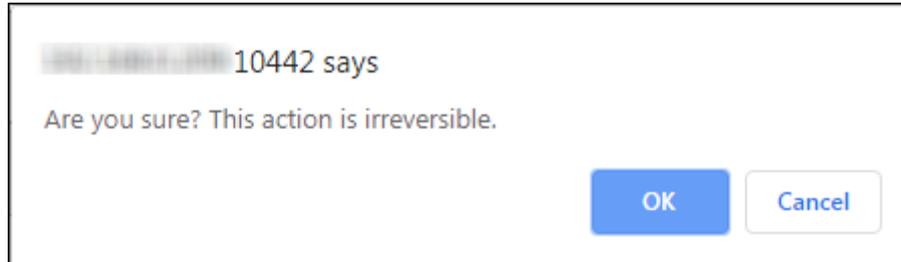
NOTE

Only JPEG, JPG, and PNG extension are supported.

Remove the Custom Header

To remove the Custom Header,

1. Go to **Administration > Customize Header**.
2. Click **Remove**.
A confirmation prompt appears.

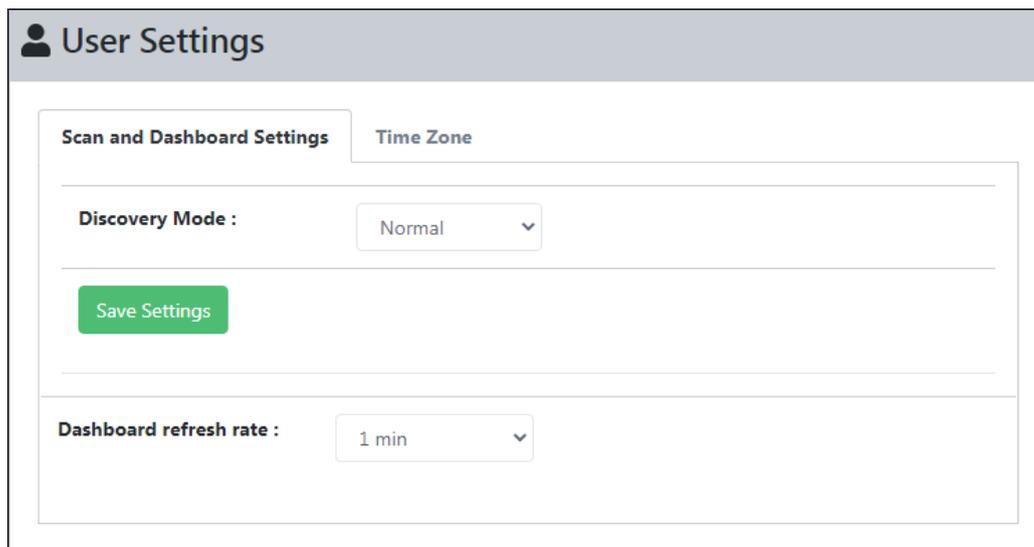


3. Click **OK**.
The custom header gets removed.

User Settings

The User Settings submodule will allow to configure the time-zone, scan and dashboard settings.

Scan and Dashboard Settings



The screenshot shows the 'User Settings' interface. At the top, there is a header 'User Settings' with a user icon. Below it, there are two tabs: 'Scan and Dashboard Settings' (active) and 'Time Zone'. Under the 'Scan and Dashboard Settings' tab, there are two sections. The first section is 'Discovery Mode' with a dropdown menu set to 'Normal'. Below this is a green 'Save Settings' button. The second section is 'Dashboard refresh rate' with a dropdown menu set to '1 min'.

Discovery Mode

This option allows the user to configure the time taken in discovery scan instead of modifying the timing individually. It has following options:

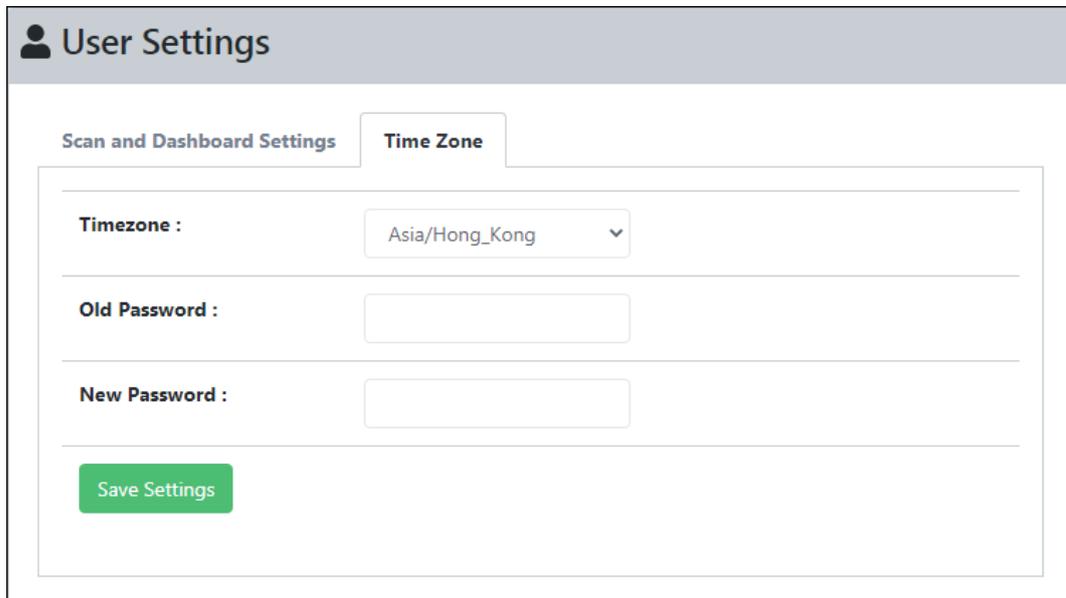
- **Polite**
- **Normal**
- **Aggressive**

After select the appropriate option, click **Save Settings**. The setting will be applied.

Dashboard refresh rate

This option allows the user to select the time to refresh the dashboard with the real-time data.

Timezone



User Settings

Scan and Dashboard Settings | **Time Zone**

Timezone : Asia/Hong_Kong ▼

Old Password :

New Password :

Save Settings

Timezone

This option allows the user to select the required timezone. UTC is the default timezone.

User can change the password that was set default for the Nemasis Console via web interface.

Old Password

Enter the old password set for the Nemasis Console.

New Password

Enter the new password that has to be set for the Nemasis Console.

Passive Scanner

The Passive Scanner module continuously monitors the activity of endpoints, ports, applications, databases, servers, and networking devices connected across network to determine its vulnerabilities in a non-intrusive manner.

It also informs if any software attempts to act as a backdoor for hackers or Trojans, which ports are open, the data being sent to, from and within, the services being run and the parts of system vulnerable to security threats.

The Passive Scanner module contains following submodules:

- Settings
- Activity Monitor
- Host
- Country
- Vulnerabilities

Settings

The Settings submodule lets you configure Passive Scanner according to your network.

⚙️ Passive Scan Settings
Start / Stop Passive Scanning : NO

Monitored Network Interfaces:

ens33

Monitored Network IP Addresses and Ranges:

192.168.0.0/24

Excluded Network IP Addresses and Ranges:

Send Event

TCP UDP

IP Address

192.168.0.30

Port

2225

Save Settings

Start/Stop Passive Scanning

Click the toggle to start/stop the passive scanning of devices connected across the network.

Monitored Network Interfaces

A network interface is a hardware or software interface between two pieces of equipment or protocol layers in a computer network. This box will display the network interfaces discovered on the Nemasis installed system. To monitor the data traffic, ensure that at least a single network interface is selected.

Clicking the anchor displays the network interface's details.

Monitored Network Interfaces:

▼ ens33

IP Address: 192.168.0.30

Netmask: 255.255.255.0

Network: 192.168.0.0

Monitored Network IP addresses and Ranges

Enter the IP addresses or ranges to be continuously monitored for passive scanning.

You can enter the IP address in the box with 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

To monitor a VLAN network, ensure you are using the syntax **vlan ipaddress/subnet**.

Excluded Network IP Addresses and Ranges

Enter the specific IP addresses or ranges to be excluded from passive scanning.

You can enter the IP address in the box with 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

To exclude a VLAN network, ensure you are using the syntax **vlan ipaddress/subnet**. If this box is left blank, all IP addresses will undergo passive scan.

Send Event

The PVS allows you to send events to an external Syslog or Security Information and Event Management (SIEM) server. You can configure it via following options:

TCP/UDP: Select the transfer protocol (TCP or UDP).

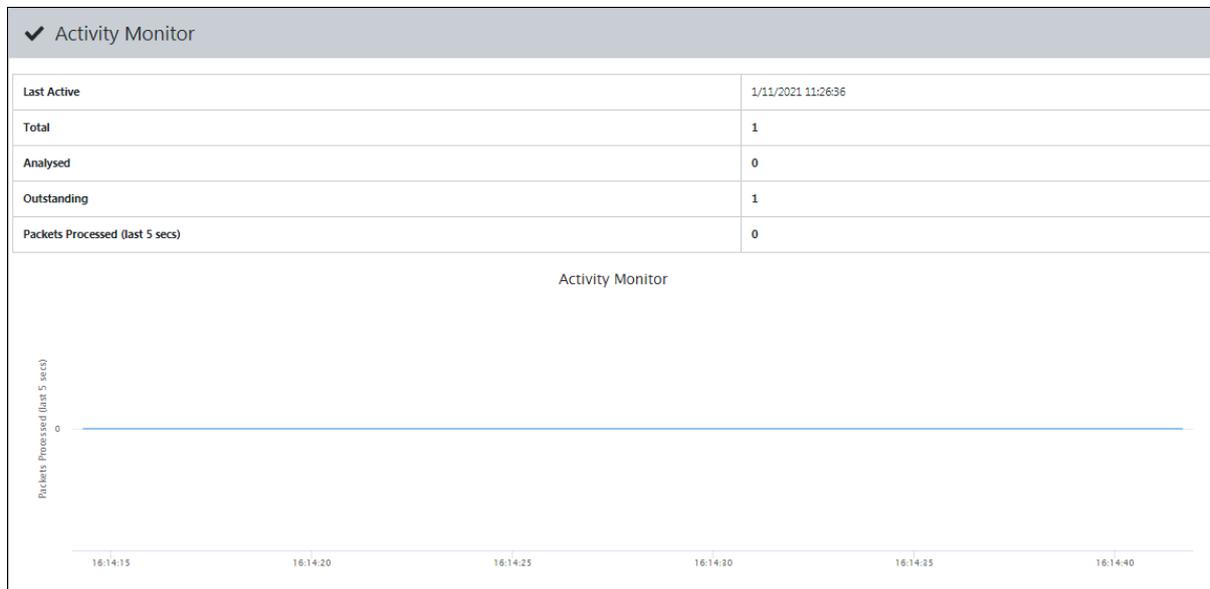
IP Address: Enter the IP Address of the receiving SIEM server.

Port Number: Enter the listening port number on the SIEM server.

After making changes, click **Save Settings**. The Passive Scanner will scan the network as per the new settings.

Activity Monitor

The Passive Scanner monitors the data packets in a network. The Activity Monitor displays the analyzed network traffic information in the form of a dynamic graph.



Last Active

It displays the last active status of the Passive Scanner in local date and time.

Total

It displays the total number of data packets.

Analyzed

It displays the number of data packets analyzed by the Passive Scanner.

Outstanding

It displays the number of data packets that are yet to be analyzed by the Passive Scanner.

Packets Processed (Last 5 secs)

It displays the number of data packets processed in last five seconds by the Passive Scanner.

Host

The Host submodule displays a list of IP addresses, its country of origin and a stacked bar chart labeled and color coded to define the number of vulnerabilities and its severity level.

Host (Passive Scan)

← 1 - 8 / 8 → 10 ▾ 1 ▾

Source IP	Country	Vulnerability / Intrusion	Total
[REDACTED]	United States	 1	1
[REDACTED]		 417728	418087
[REDACTED]		 15346268	15375668
[REDACTED]		 330916567	330936833
[REDACTED]		 18	18

Source IP

This column displays the IP address of endpoint sending malicious data packets to other endpoints connected across the network.

Country

This column displays the country of origin of the public IP address. Users should note that country will be displayed only for public IP addresses.

Vulnerability/Intrusion and Total

Clicking the Vulnerability/Intrusion chart or numerical value in Total column displays the vulnerability's name and total number of malicious attempts made by it.

Source IP: [REDACTED] ×

> OS-WINDOWS Microsoft Windows RDP MS_T120 channel bind attempt 28

Close

Clicking the vulnerability displays following details:

- First and last observation of the vulnerability by passive scanner.
- References for the vulnerability.
- Ports used to send malicious data packets to the target IP addresses and Ports

Source IP: [REDACTED] ×

▼ OS-WINDOWS Microsoft Windows RDP MS_T120 channel bind attempt 28

First Observed: Jul 03 2019 12:11 PM Last Observed: Jul 03 2019 12:11 PM

See References

<http://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0708>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-0708>

59703/TCP	→	[REDACTED]:3389
59705/TCP	→	[REDACTED]:3389
59745/TCP	→	[REDACTED]:3389
59736/TCP	→	[REDACTED]:3389
59822/TCP	→	[REDACTED]:3389
Show More...		

Close

Country

The Country submodule displays the country of intrusive public IP address, vulnerability/intrusion bar and total number of times it sent malicious data packets.

Country (Passive Scan)		
Country	Vulnerability / Intrusion	Total
United States		1
Netherlands		1

Vulnerability/Intrusion

Clicking the bar chart displays the list of public IP addresses and total number of malicious attacks attempted. The different sections in bar will display different findings. For example, clicking the Red section of the India's bar chart displays only the Red section's findings.

Country: India	
> 	4777
> 	1
> 	139

[Close](#)

Clicking the IP address box further displays the vulnerability, first and last observation, references, source Port number, destination IP address and Port number.

Country: India ×

▼ [Redacted IP] 4777

INDICATOR-SHELLCODE x86 inc ecx NOOP

First Observed: Jul 03 2019 12:18 PM *Last Observed: Jul 03 2019 12:18 PM*

50730/TCP → [Redacted IP]:143

> [Redacted IP] 1

> [Redacted IP] 139

Close

Total

Clicking the numerical value in Total column displays a list of public IP addresses and malicious attacks attempted by them.

Vulnerabilities

The Vulnerabilities submodule displays the vulnerabilities detected in descending order of severity. It also displays vulnerability's name, its first and last observation, references and total number of times it sent malicious data packets.

Vulnerabilities (Passive Scan)				
Vulnerability / Intrusion	First Seen	Last Seen	References	Total
DNS Reply Detected	Apr 15 2020 08:20 PM	Apr 15 2020 08:20 PM	0	40985
DNS Request Detected Any	Apr 15 2020 07:45 PM	Apr 15 2020 07:45 PM	0	346730615

References

Clicking the numerical value in References column displays various references for the vulnerability.

References: INDICATOR-SHELLCODE ssh CRC32 overflow filler ×

See References

- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0572>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0144>
- <http://www.securityfocus.com/bid/2347>

Close

Total

Clicking the numerical value in Total column displays the IP addresses and total number of times malicious data packets sent.

Vulnerability: INDICATOR-SHELLCODE ssh CRC32 overflow filler ×

> [IP Address] 3

> [IP Address] 2

Close

Clicking the IP address box further displays the source Port number, destination IP address and Port number.

Vulnerability: INDICATOR-SHELLCODE ssh CRC32 overflow filler ×

▼ [IP Address] 3

60960/TCP	→	[IP Address]:22
60962/TCP	→	[IP Address]:22
60964/TCP	→	[IP Address]:22

> [IP Address] 2

Close

License

The License module 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 new license.

[Enter Subscription Key](#) [Buy Now](#)

🔑 Subscription Details

Subscription Status	Trial
Subscription Expiry	2024-12-31
Total Assets	15
Scanned Assets	1
Branch Code	1234567890123456789012345678901234

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.

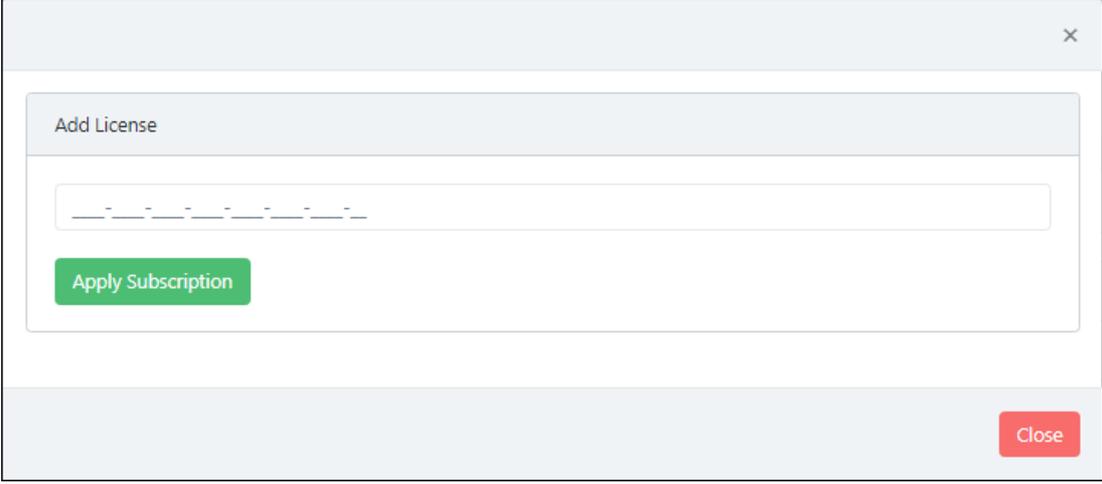
Branch Code

It is a unique code that defines the respective instance.

Enter Subscription Key

To enter the Subscription Key,

1. Go to **License > Subscription Details**.
2. Click **Enter Subscription Key**.
Add License window appears.



3. Enter the subscription key.
4. Click **Apply Subscription**.
A message appears displaying successful subscription.

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, then you will have to buy a new license. To buy a new license, click **Buy Now**.

Manage Instance

The Manage Instance module lets you to import and export the Nemasis instance. It also has Two Factor Authentication along with lets user to get offline updates. The Manage Instance contains following submodules:

- **Two-Factor Authentication (2FA)**
- **Import & Export**
- **Offline Updates**
- **System Information**
- **Whitelisted IP**

Two-Factor Authentication (2FA)

The system login password is Single-Factor Authentication which is considered unsecure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your basic system login.

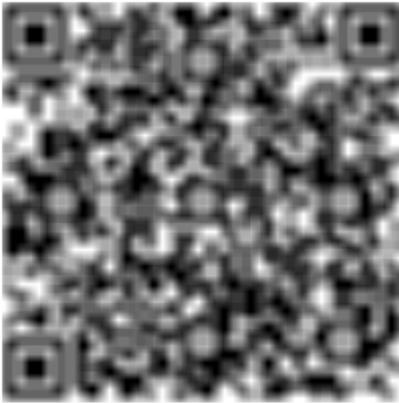
The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering Nemasis credentials. So, even if somebody knows your Nemasis credentials, the 2FA feature secures data against unauthorized logins.

Only administrator can enable/disable the 2FA feature. It can also be enabled for added users as well.

Two Factor Authentication

Enable / Disable [Manage Other User Settings](#)

Scan QR Code



OR

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Enable Two Factor Authentication

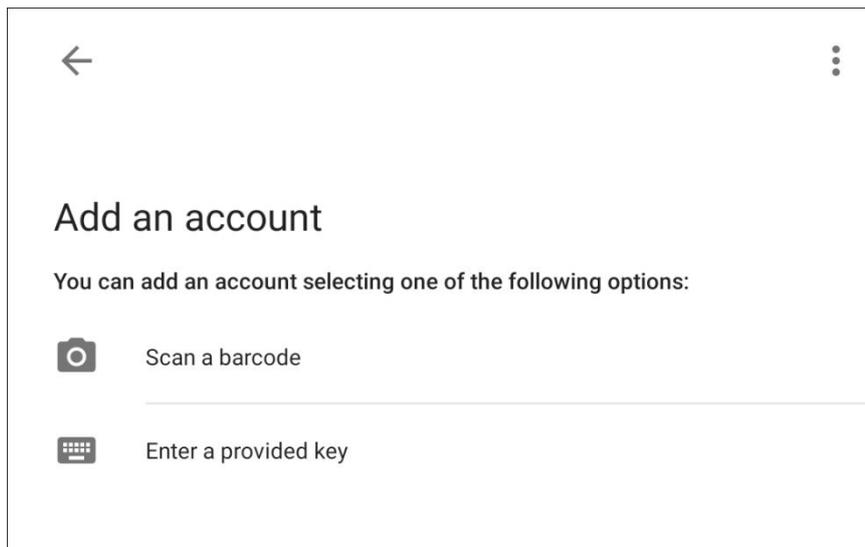
Note: Please make sure client device time is correct or codes generated in app will not be validated.

 NOTE	Ensure that the smart device's date and time matches with the system's date and time or else TOTP's generated by app won't get validated.
----------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------

Enable 2FA login

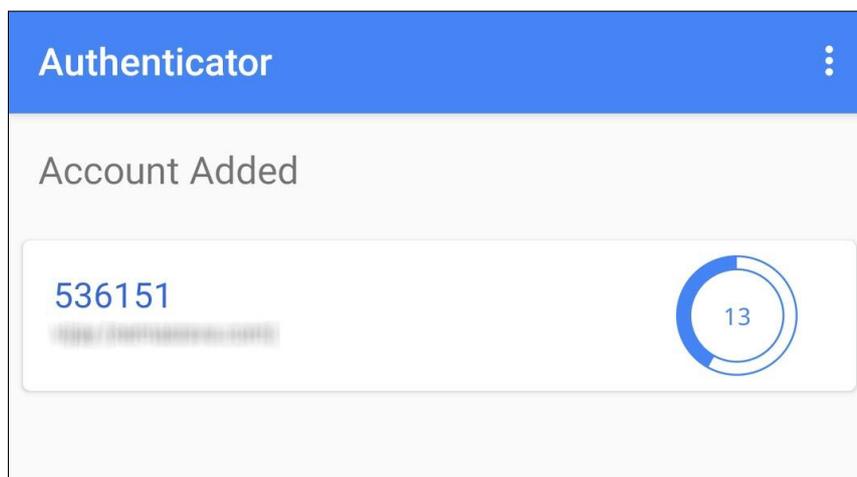
To enable 2FA, follow the steps given below:

1. Install the Authenticator app for Android devices from Play Store or for iOS devices from App Store on your smart device.
2. Open the Authenticator app.
After basic configuration following screen appears.



3. Select a preferred option. If you tapped **Scan a barcode**, scan the onscreen QR code via your smart device. If you tapped **Enter a provided key**, enter the Account Key and then tap **ADD**.

After scanning the Account QR code or entering Account Key the Nemasis server account gets added to the Authenticator app. The app then starts displaying a Time-based One-Time Password (TOTP) valid for 30 seconds.

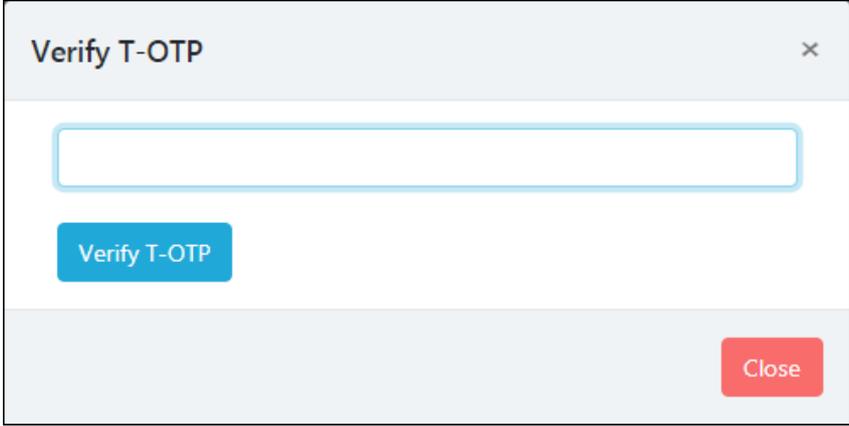


TIP

We recommend that you store the Account Key in offline storage or a paperback copy, in case you lose the account access.

4. Click **Enable Two-Factor Authentication**.

Verify TOTP prompt appears.

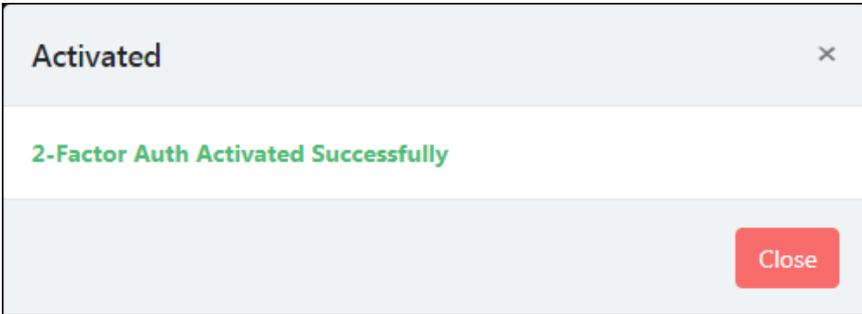


A dialog box titled "Verify T-OTP" with a close button (X) in the top right corner. It contains a text input field with a light blue border. Below the input field is a blue button labeled "Verify T-OTP". In the bottom right corner, there is a red button labeled "Close".

5. Enter the TOTP displayed on smart device.

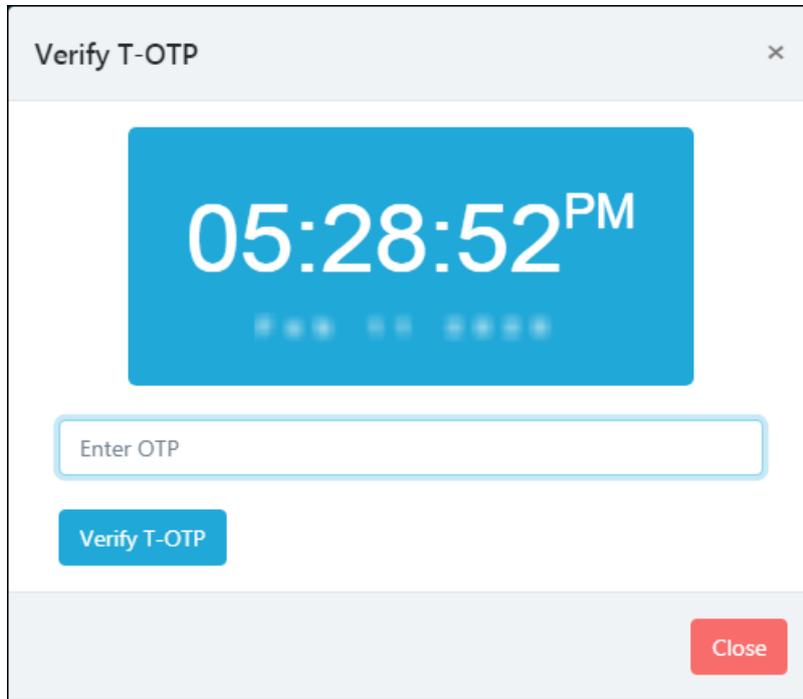
6. Click **Verify TOTP**.

After entering the correct TOTP, the 2FA feature gets enabled and following success message appears.



A dialog box titled "Activated" with a close button (X) in the top right corner. It displays a green success message: "2-Factor Auth Activated Successfully". In the bottom right corner, there is a red button labeled "Close".

After enabling the 2FA feature, whenever you log in to Nemasis, Verify TOTP screen appears.



The screenshot shows a modal window titled "Verify T-OTP" with a close button (X) in the top right corner. The main content area features a large blue rectangle displaying the time "05:28:52^{PM}" and a row of six dots below it, representing a TOTP code. Below this is a text input field with the placeholder "Enter OTP". Underneath the input field is a blue button labeled "Verify T-OTP". At the bottom right of the modal is a red button labeled "Close".

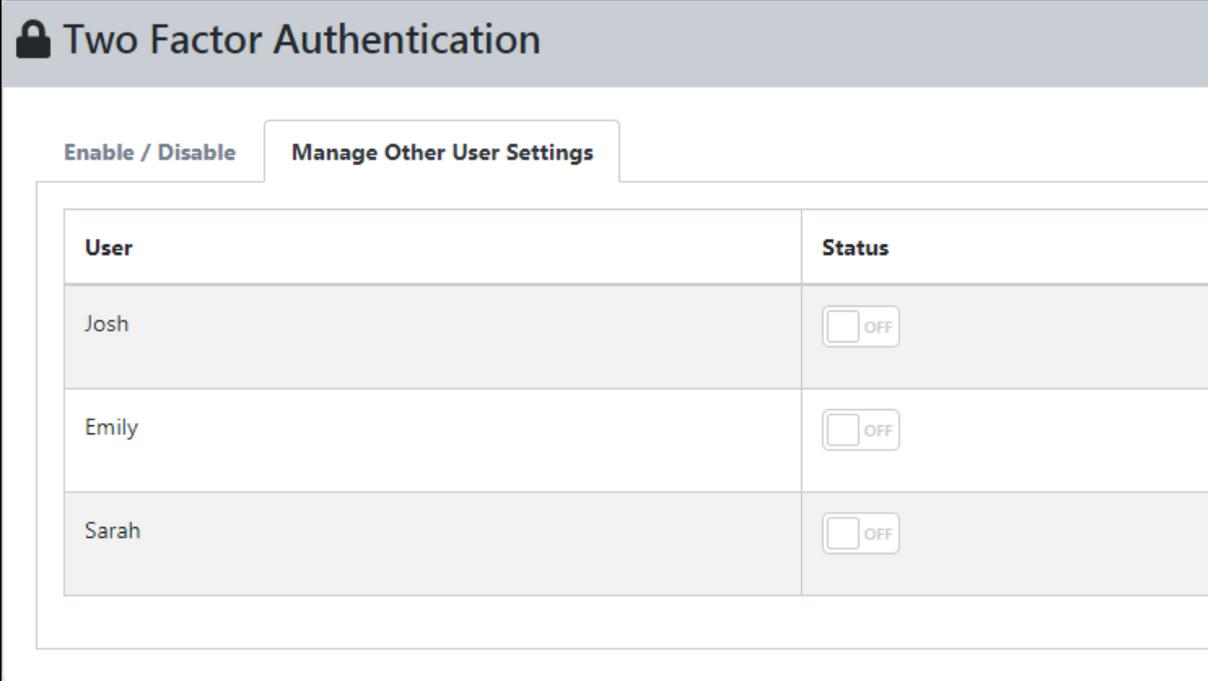
Enter the TOTP displayed in Authenticator app and click **Verify TOTP**.
The Nemasis admin account is now protected with 2FA login.

Enable 2FA login for added users

After enabling the 2FA feature, you can also enable 2FA login for added users.

To enable 2FA login for added users, follow the steps given below:

1. Go to **Manage Instance > Two Factor Auth.**
2. Click **Manage Other User Settings** tab.
The tab displays list of added users and whether 2FA status is enabled or disabled.



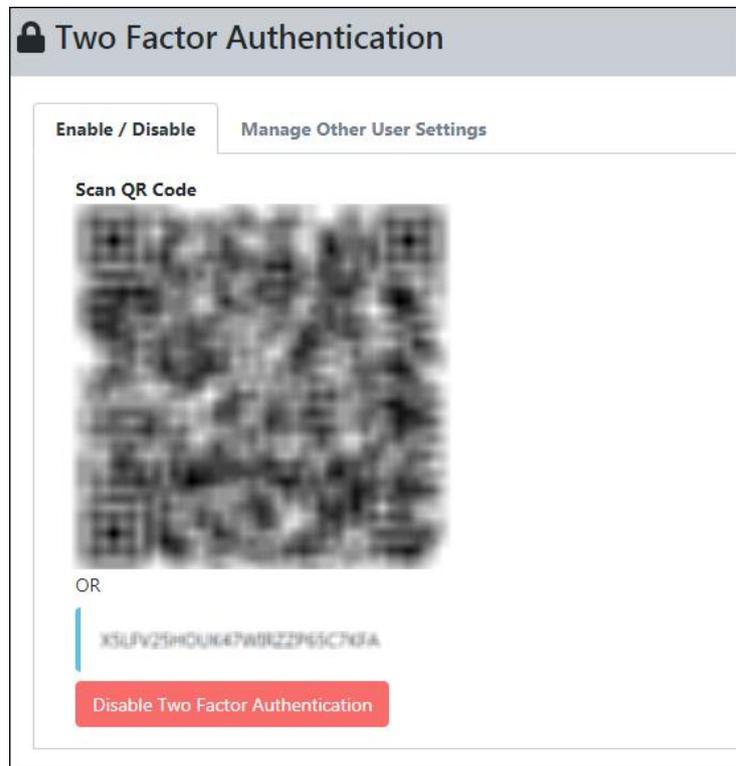
User	Status
Josh	<input type="checkbox"/> OFF
Emily	<input type="checkbox"/> OFF
Sarah	<input type="checkbox"/> OFF

3. To enable 2FA login for a user, click the toggle button to **ON** state.
The 2FA login for added users gets enabled.

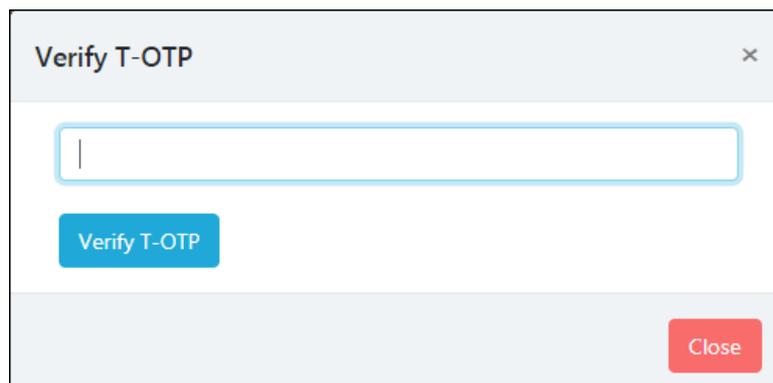
Disable 2FA login

To disable 2FA login, follow the steps given below:

1. Go to **Manage Instance > Two Factor Auth.**
2. Click **Disable Two-Factor Authentication.**

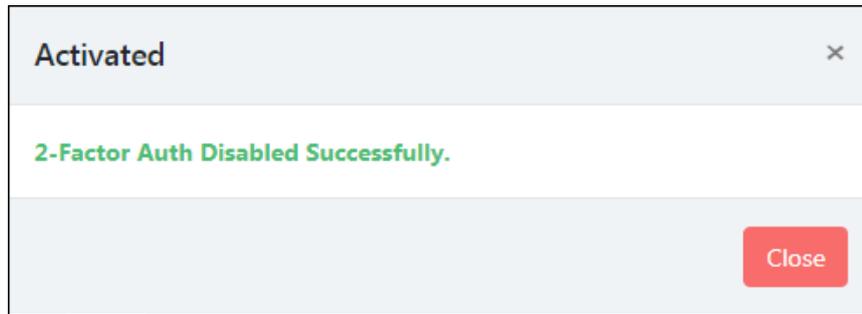


Verify TOTP window appears.



3. Enter the TOTP.
4. Click **Verify T-OTP.**

The 2FA feature gets disabled.



 NOTE	After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated for added users.
--------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------

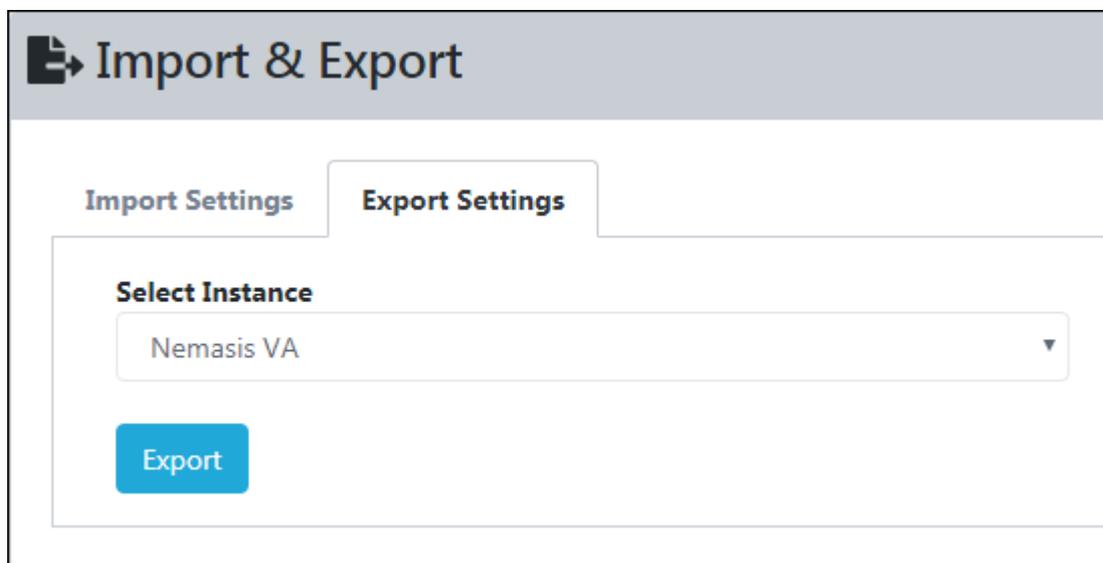
Import & Export

The Import & Export submodule lets you import and export a Nemasis instance. This feature lets you create a backup of the instance data and restore it in case of any disaster management, maintenance, or undesirable events.

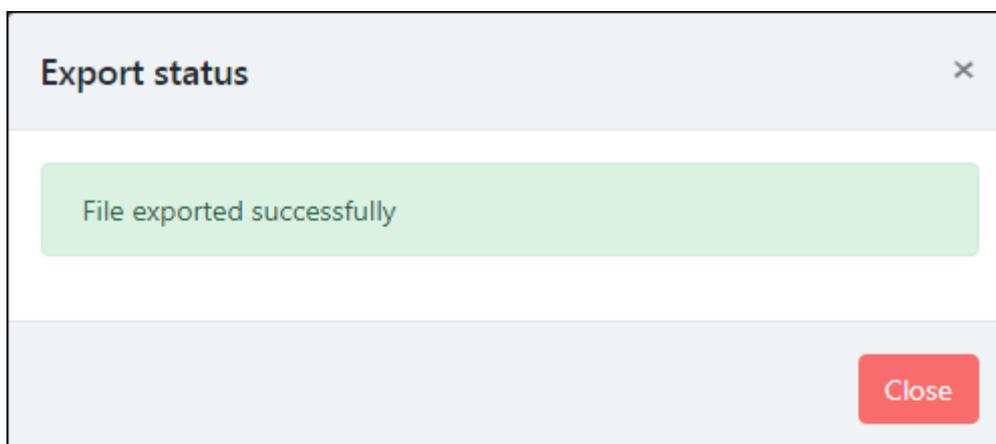
Export an Instance

To export an instance,

1. Go to **Manage Instance > Import & Export**.
2. Click the **Export Setting** tab.
3. Click the Select Instance drop-down and select the preferred instance.



4. Click **Export**.
After the export process is complete, following message appears.

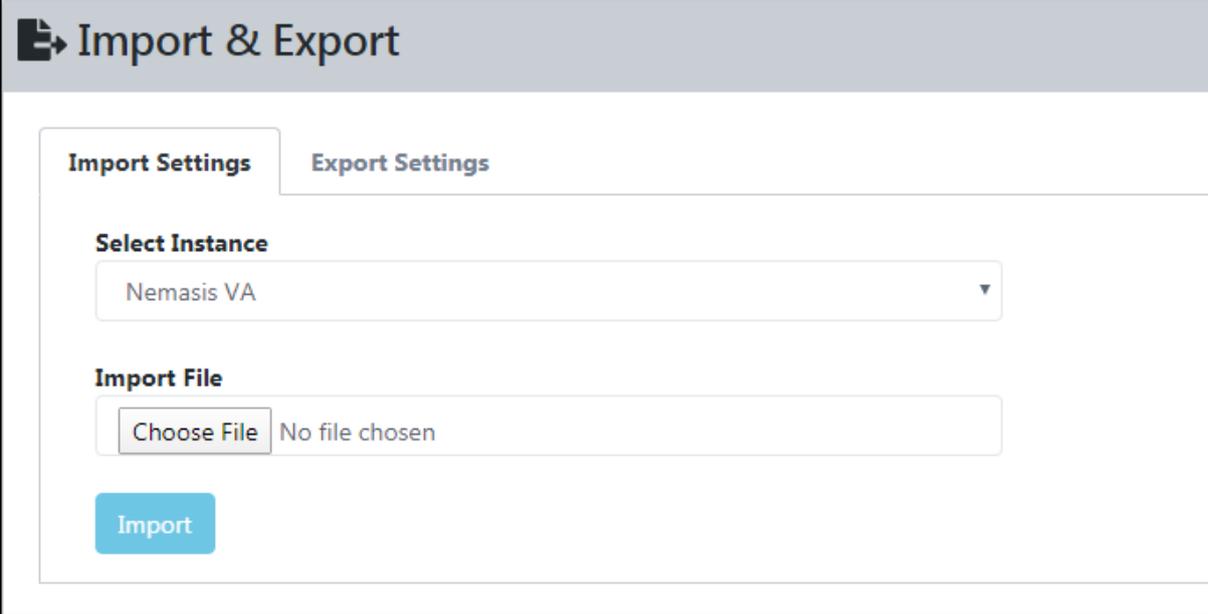


5. After the file is exported is successfully, you can download the file by clicking [📄 Click here to download exported file.](#)

Import an Instance

To import an instance,

1. Go to **Manage Instance > Import & Export**.
2. Click **Select Instance** drop-down and select an instance.



Import & Export

Import Settings | **Export Settings**

Select Instance

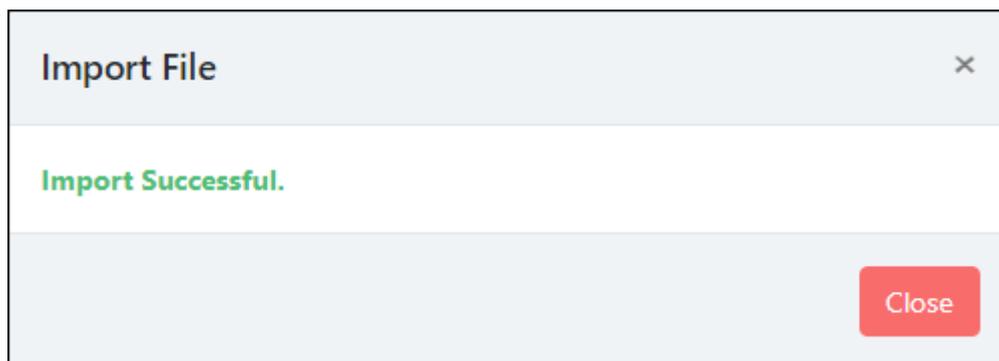
Nemasis VA

Import File

Choose File No file chosen

Import

3. Click **Choose File** and select a file to be imported.
 4. Click **Import**.
- After the import process is complete, following message appears.



Offline Updates

The **Offline Updates** submodule lets you update Nemasis instance in offline mode for air-gapped system. You can download the update/upgrade file from internet and update the Nemasis instance offline. With Offline Updates, you can update/upgrade the Nemasis instance even if Nemasis trial period is over or license has expired.



Depending upon the component change, a running task may get interrupted.

Offline Updates

Select File

Choose File No file chosen

Upload Update File

Upload Offline Updates

To upload the offline updates,

1. Download the [offline updates file](#) (zip format).
2. Go to **Manage Instance > Offline Updates**.
3. Click **Choose File** and select the downloaded file.
4. Click **Upload Update File**.

Nemasis instance update initiates.

TIP

You can bookmark or share the following link to download Offline Updates:
https://download1.mwti.net/nemasis/nemasis_update.zip

System Information

The System Information submodule displays detailed information of the Nemasis installed system. You can view General, Boot Time, CPU, Memory, Disk, and Network information.

System Information

General

System	Linux
Hostname	nemasis
Release	4.9.0-12-amd64
Version	#1 SMP Debian 4.9.210-1 (2020-01-20)
Machine	x86_64

Boot Time

Formatted	Jan 02 2021 01:36 PM
System Up Time	460:22:40

CPU Information

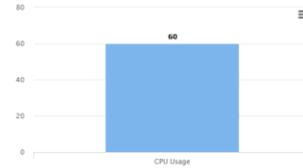
Physical Cores	2
Logical Cores	4
Current Frequency	3392.00MHz

CPU Usage Information:

Current Frequency	3392.00MHz
-------------------	------------

CPU Usage Information:

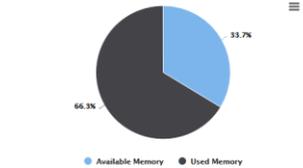
Core0	100.0
Core1	0.0
Core2	66.7
Core3	100.0
Total CPU Usage	60.0%



Memory Information

Physical Information:

Total	3.85GB
Available	1.22GB
Used	2.40GB
Percentage	68.30%



Swap Information:

Total	Available	Used	Percentage
4.00GB	3.46GB	552.96MB	13.508%

Disk Information

Partitions and Usage Information:

Device	/dev/sda1
Mountpoint	/
File System Type	ext4
Mountpoint	/
File System Type	ext4
Total Size	74.31GB
Used	47.48GB
Free	23.01GB

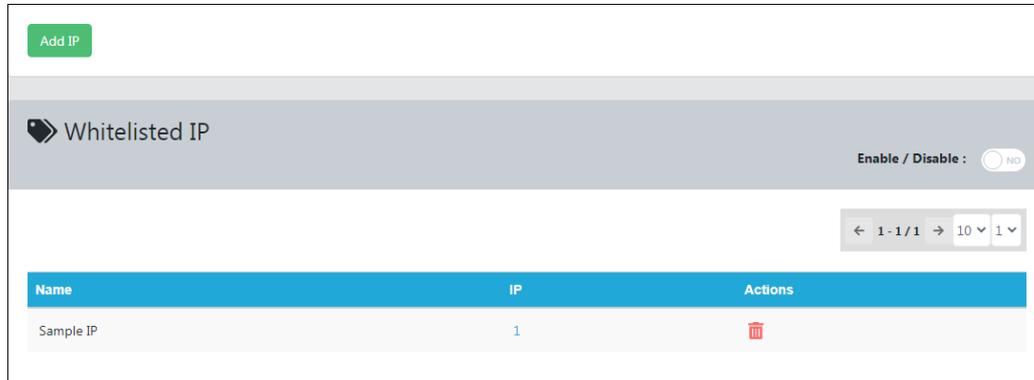
Total Read	Total Write
71.89GB	409.29GB

Network Information

Interface Name	ens33
IP Address	192.168.1.100
Netmask	255.255.255.0
Broadcast IP	192.168.1.255
Total Bytes Sent	9.81GB
Total Bytes Received	11.00GB

Whitelisted IP

This module allows the user to add IP addresses only that can take access the Nemasis Console.

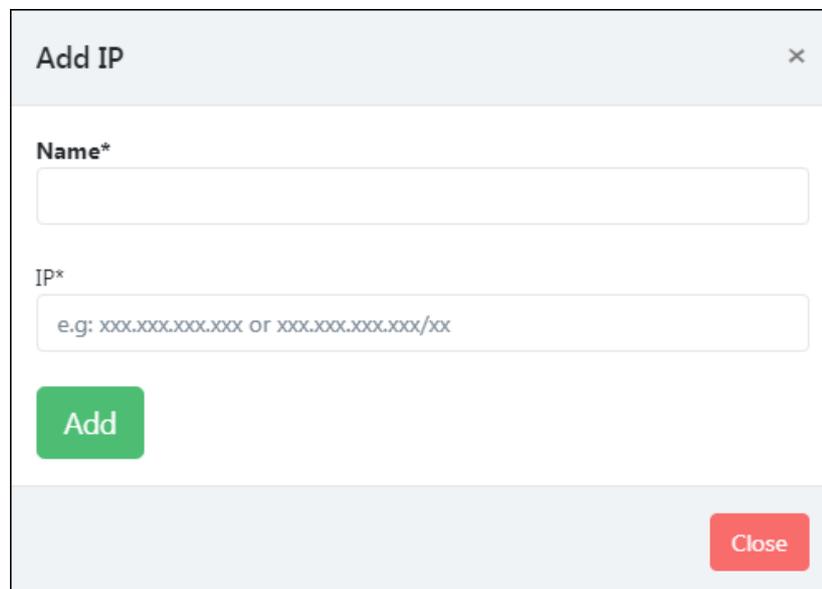


Add a Whitelisted IP

To add a Whitelisted IP,

1. Go to **Manage Instance > Whitelisted IP**.
2. Click **Add IP**.

Add Scanner window appears.



The screenshot shows a modal window titled 'Add IP' with a close button (X) in the top right corner. The form contains two input fields: 'Name*' and 'IP*'. The 'IP*' field has a placeholder text: 'e.g: xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/xx'. Below the input fields is a green 'Add' button. At the bottom right of the modal is a red 'Close' button.

3. Enter an appropriate name.
 4. Enter the IP address.
 5. Click **Add**.
- The IP address gets added to the Whitelisted IP list.

Actions

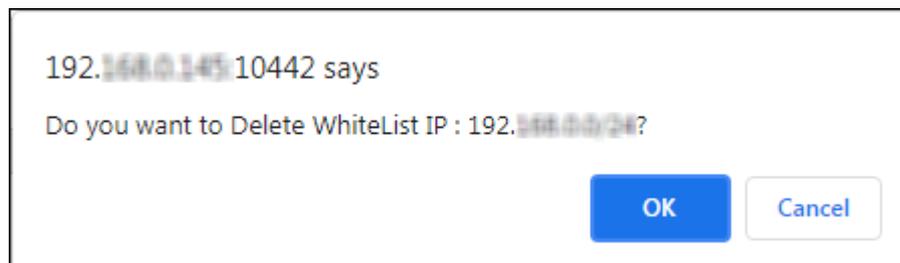
Clicking icons in the Actions column lets you take actions regarding an Whitelisted IP.

-  Delete Whitelisted IP

Delete an IP

To delete an IP,

1. Go to **Manage Instance > Whitelisted IP**.
2. In the **Actions** column, click .
A confirmation prompt appears.



3. Click **OK**.
The Whitelisted IP gets deleted.

Audit Trail

You can view the detailed analysis of particular system by using the IP address of it. You can also filter it based on the date and month on which audit was performed.

Search audit trail by IP address

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

Audit Trail

From Date *  **To Date *** 

IP
192.168.0.245
192.168.0.228
192.168.0.78
192.168.0.44

- From the list, click on the IP address for which you want to view the report.
The detailed audit report will be generated.

Audit Trail For IP : 192.168.0.228

Export

1 - 10 / 43 10 1

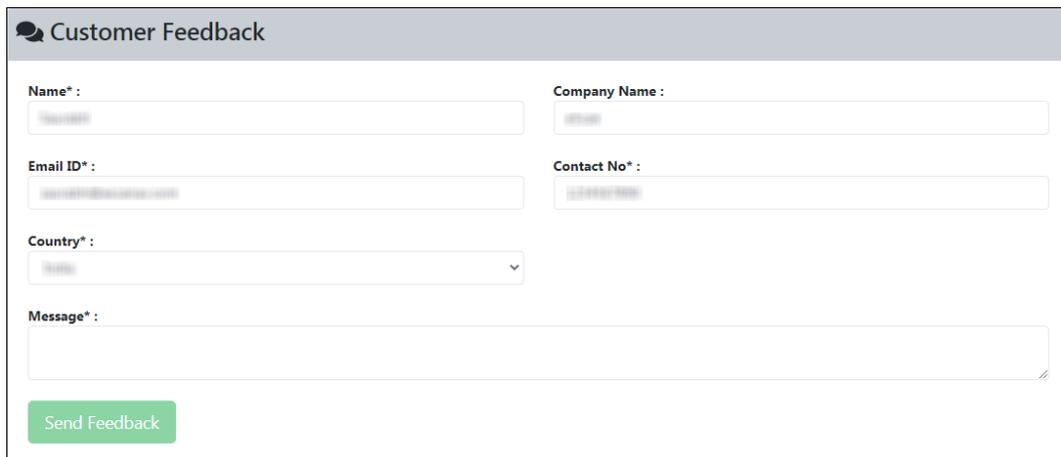
Time	User	Action	Command
Aug 06 2021 12:09 PM	admin	License :: Subscription Details	Viewed License Details.
Aug 06 2021 12:09 PM	admin	admin	Logged In
Aug 06 2021 12:08 PM	admin	Reports	Viewed Reports Details.
Aug 06 2021 12:07 PM	admin	port_list	Viewed port_list Details.
Aug 06 2021 11:57 AM	admin	target	Viewed target Details.
Aug 06 2021 11:56 AM	admin	credential	Viewed credential Details.
Aug 06 2021 11:56 AM	admin	port_list	Viewed port_list Details.
Aug 06 2021 11:56 AM	admin	target	Viewed target Details.
Aug 06 2021 11:56 AM	admin	Task Results :: Vulnerabilities	Viewed Vulnerabilities Details.
Aug 06 2021 11:56 AM	admin	result	Viewed result Details.

Help & Support

The Help and Support module contains **Feedback** and **Support Request** submodules. Your personal details submitted at the time of registration are autofilled by Nemasis. These details can be modified.

Feedback

The Feedback submodule lets you send a feedback about Nemasis.



The form is titled "Customer Feedback" and contains the following fields:

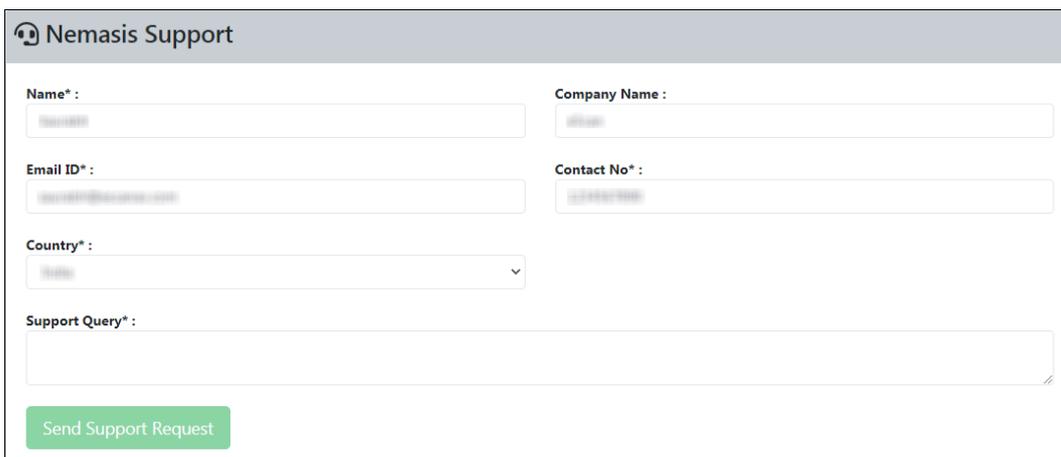
- Name* :
- Company Name :
- Email ID* :
- Contact No* :
- Country* :
- Message* :

A green button labeled "Send Feedback" is located at the bottom left of the form.

Enter your feedback in the Message box and then click **Send Feedback**.

Support Request

The Support Request submodule lets you send a support request to the Support team.



The form is titled "Nemasis Support" and contains the following fields:

- Name* :
- Company Name :
- Email ID* :
- Contact No* :
- Country* :
- Support Query* :

A green button labeled "Send Support Request" is located at the bottom left of the form.

Enter your message in the Support Query box and then click **Send Support Request**. After receiving the support request, the Nemasis Support Team will get in touch with you as soon as possible.

Contact Us

We provide 24/7 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 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
- Step-by-step description of troubleshooting if any attempted
- Screenshots, error messages, and log files

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

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

Chat Support

The Nemasis technical support team is available round-the-clock to assist you with your queries. You can contact our support team via [live chat](#).

Email Support

If you have any queries, suggestions, or comments regarding Nemasis or this User Guide, write to our [Support team](#).