



COMODO
Creating Trust Online®

COMODO
one

Comodo One

Software Version 3.29

Network Assessment Tool Quick Start Guide

Guide Version 1.3.010820

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo One - Network Assessment Tool - Quick Start Guide

This tutorial briefly explains how an admin can setup Comodo Network Assessment Tool (NAT) and run assessment scans on the network.

Basic Setup:

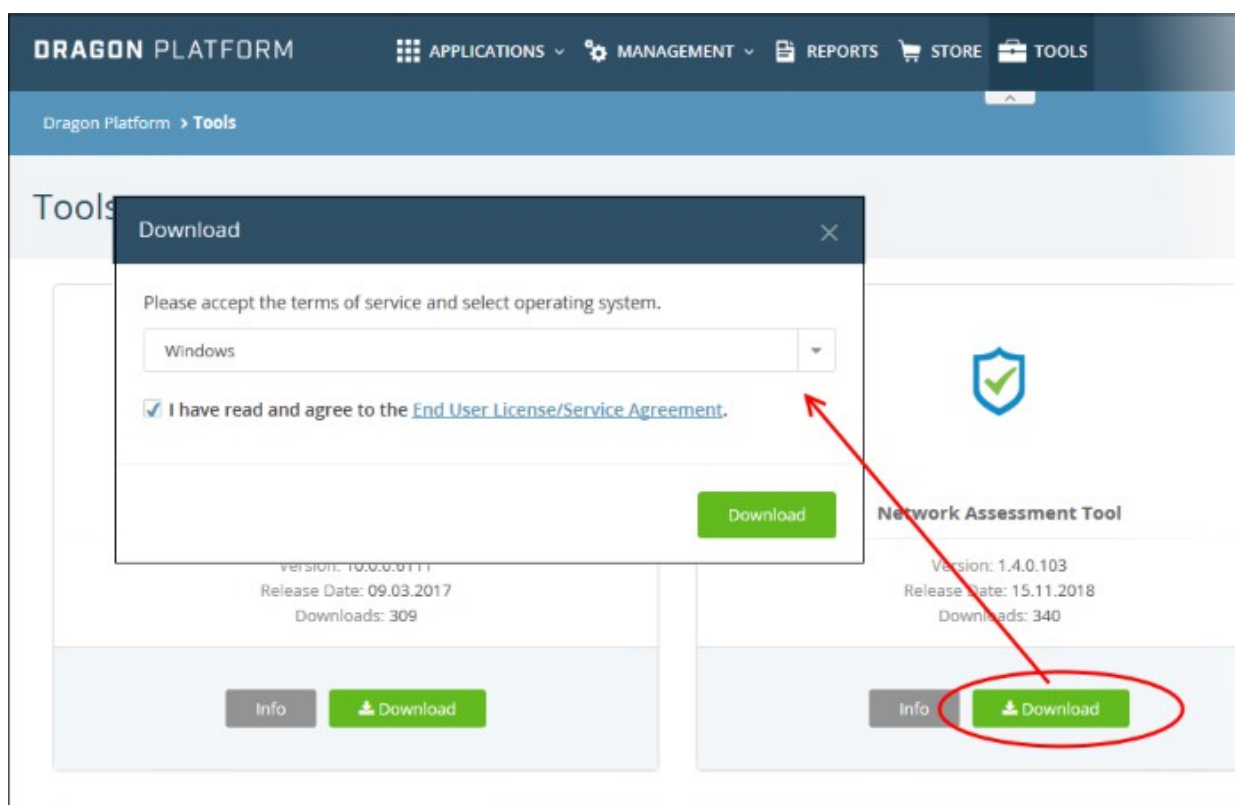
- Install the NAT tool and run the initial configuration wizard. The wizard allows you to enable scanning your domain/workgroup/IP Address Range, to which your computer is a member of and specify the administrative credentials for NAT to access the endpoints on your network.
- Add additional domains/workgroups/IP Address Ranges, accessible by your computer for scanning
- Enter login credentials with administrative privileges for the added networks and map them to respective networks

The guide will take you through the basic setup and usage of Comodo NAT. Click any link to go straight to the section you need help with.

- [Step 1 - Login to Comodo One and download the NAT Tool](#)
- [Step 2 - Install NAT Tool](#)
- [Step 3 - Run Initial Configuration Wizard](#)
- [Step 4 - Add Networks](#)
- [Step 5 - Add Credentials and Map to Respective Networks](#)
- [Step 6 - Run a Scan](#)
- [Step 7 - Generate Reports](#)

Step 1 - Login to Comodo One and download the NAT Tool


- Login to your Comodo One account at <https://one.comodo.com/app/login>
- Click 'Tools' on the top-menu.
- Click 'Download' in the 'Network Assessment Tool' tile:



- Agree to the EULA then click the 'Download' button

Step 2 - Install NAT Tool

Prerequisite - To work correctly, NAT requires that Network Mapper (NMAP) and Microsoft Baseline Security Analyzer (MBSA) are also installed. The installation wizard will allow you to download both applications if you do not have them already.

- Double click on the setup file  to start the NAT installation wizard
- Follow the wizard and continue the installation.

On completion of installation, the wizard will check whether the prerequisite software MBSA and NMAP are installed.

- If available, the installation will complete and will move to the **initial configuration wizard**.



END USER LICENSE AGREEMENT AND TERMS OF SERVICE
COMODO ONE STANDARD MODULE
COMODO NETWORK ASSESSMENT TOOL

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO ONE MODULE SOFTWARE PRODUCT (THE "PRODUCT"). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE SOFTWARE, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON "I ACCEPT".

Product Functionality

For a complete list and description of the Product features and functions, please refer to the appropriate section of any applicable Administration Guide.

This end user license and subscriber agreement is between you ("you" or "Subscriber"), an individual, and Comodo Security Solutions, Inc., a Delaware company, with offices at 1255 Broad Street, Clifton, NJ 07013, United States (hereinafter referred to as "Comodo").

In exchange for your use of the Product, you agree as follows:

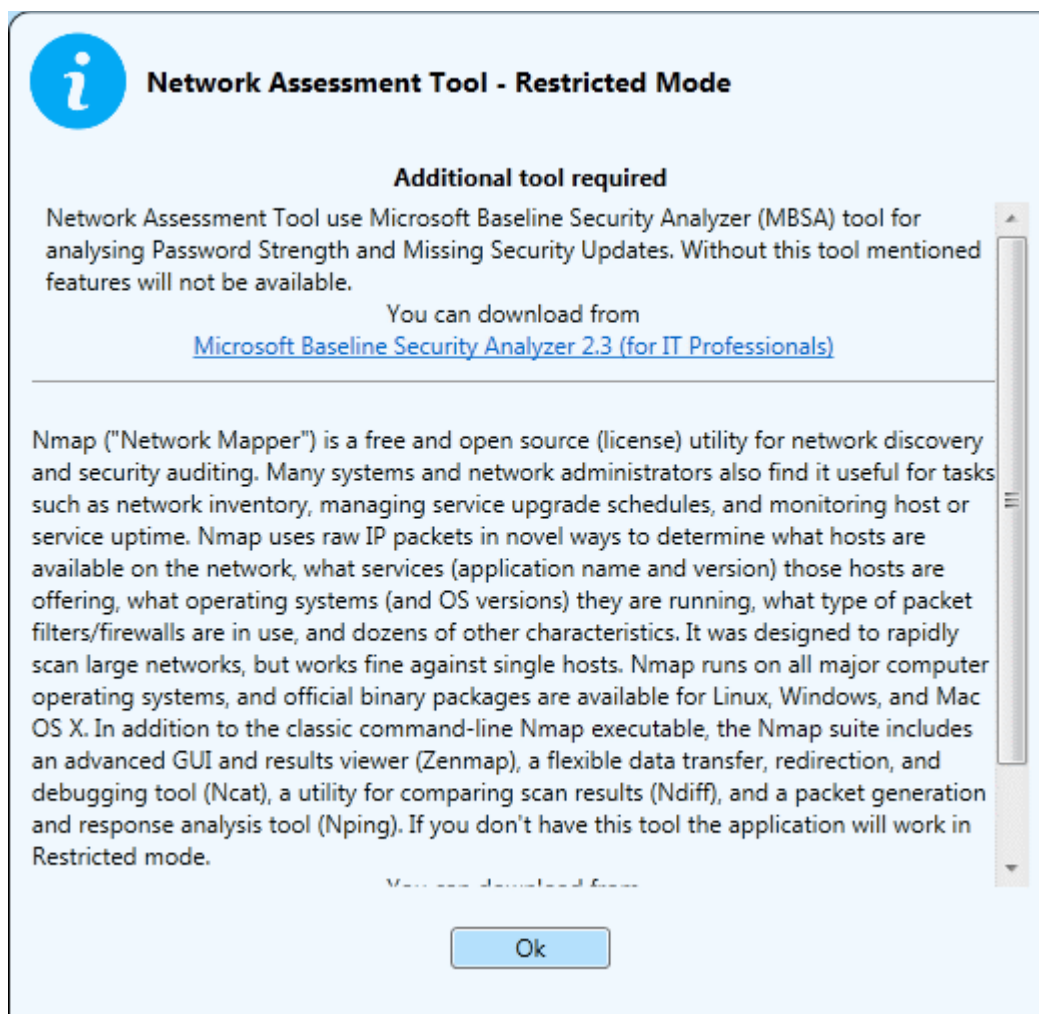
1. License

1.1. Grant of License.

Comodo grants you a limited, non-exclusive, non-transferable, and revocable user license to download, install, back-up, and use the Software (collectively, the "Product"), including any documentation and files accompanying the Product. You shall not resell, lease, sell, modify, reverse engineer, conduct tests, decompile, or create derivative works of the Software. All rights not expressly granted herein are reserved to Comodo.

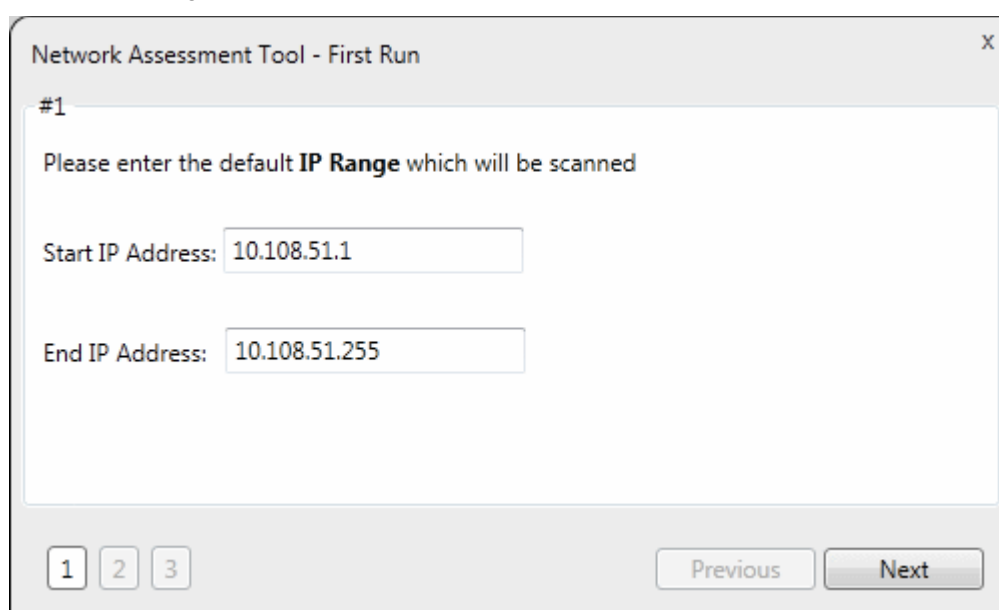
This License grant shall expire at the end of the paid subscription period or at the end of the trial period.

- Agree to the terms and conditions and follow the steps in the installation wizard.
- The wizard will check whether the required NMAP and MBSA software are installed.
 - If they are installed, NAT installation will complete and you'll move to the **initial configuration wizard**.
 - If they are not installed, you will see a dialog with download links for the tools. Follow the instructions and install the two tools:



Step 3 - Run Initial Configuration Wizard

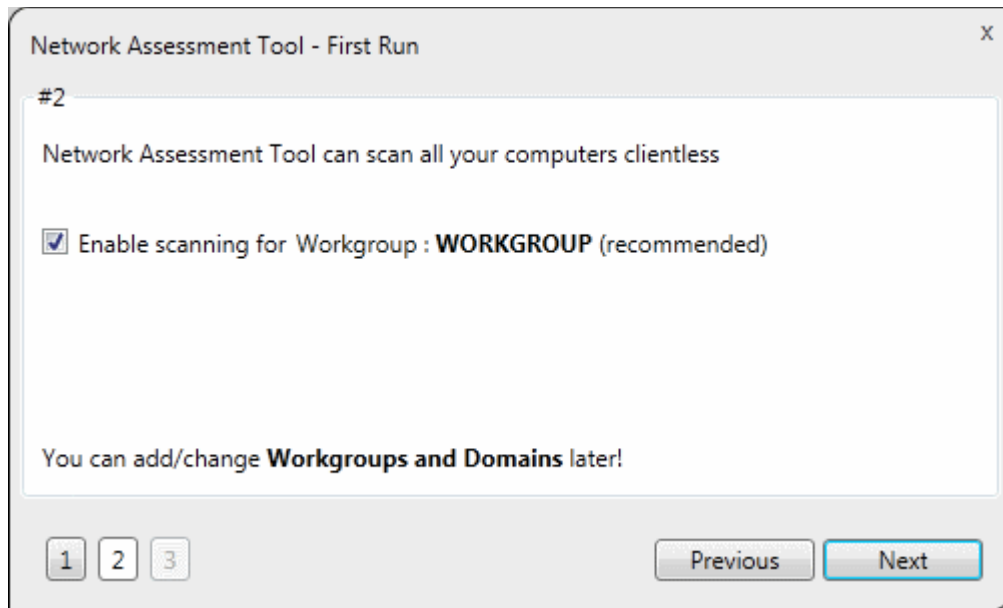
The configuration wizard begins once NAT installation is complete:



NAT automatically identifies the workgroup or domain to which your computer is a member of and displays it.

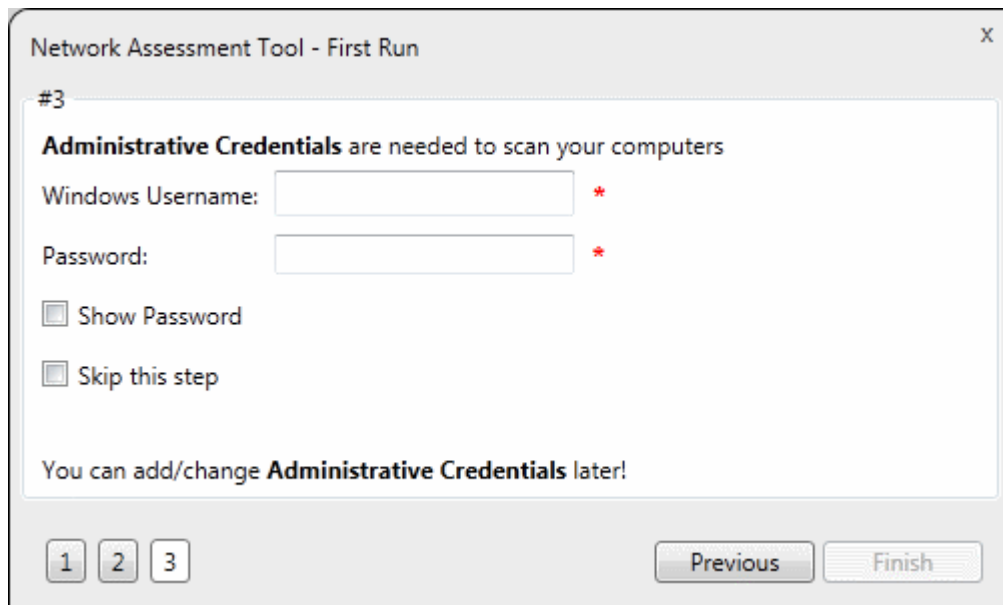
- Select 'Enable scanning Workgroup/Domain' if you want to automatically add workgroup/domain

- Click 'Next'.

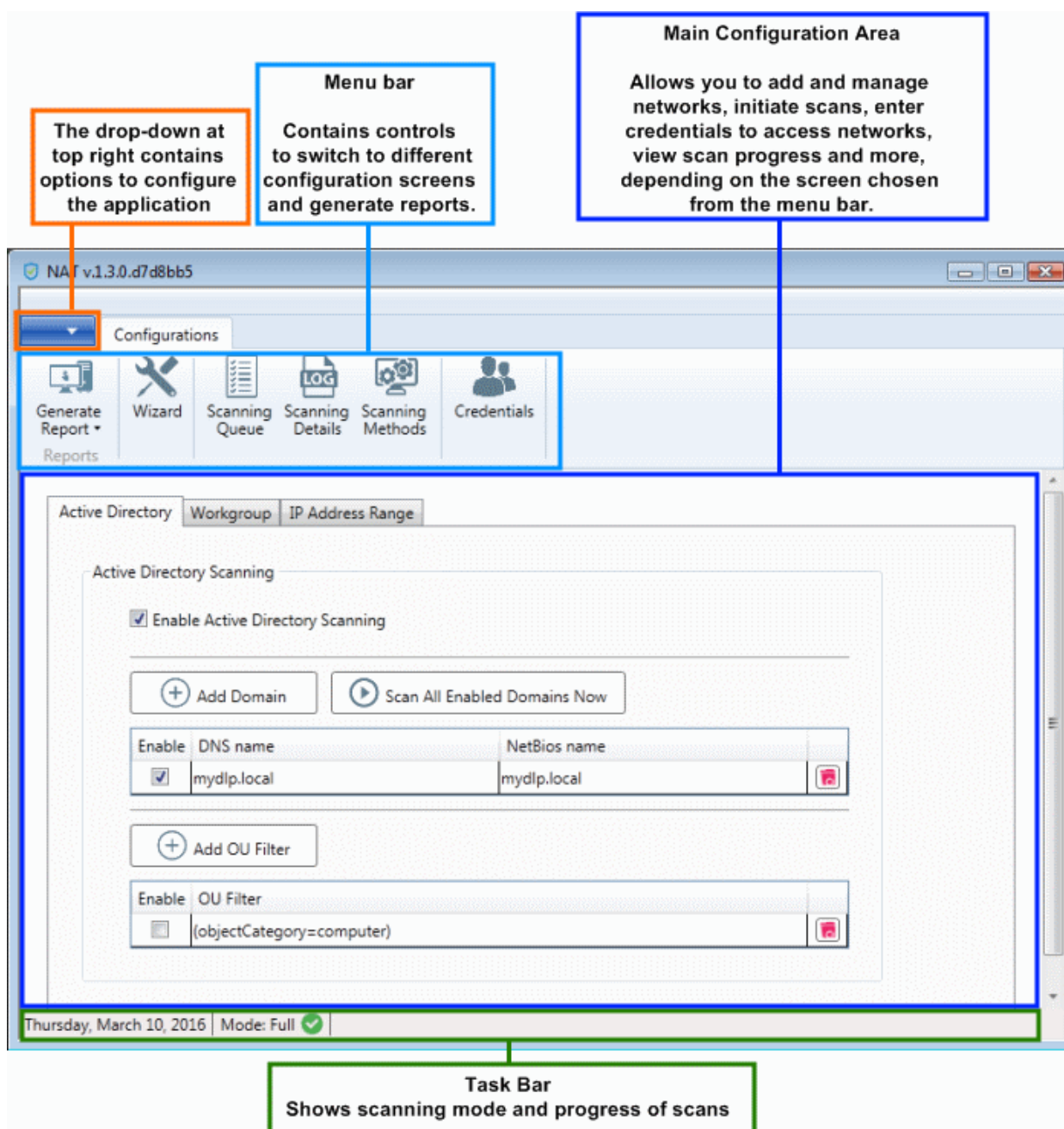


NAT automatically identifies the workgroup or domain to which your computer is a member of and displays it.

- Select 'Enable scanning Workgroup/Domain' if you want to automatically add workgroup/domain
- Click 'Next'



- Enter an admin username and password for the target network and click 'Finish'.
- NAT will immediately begin scanning your network. Progress is shown at the bottom of the main interface:



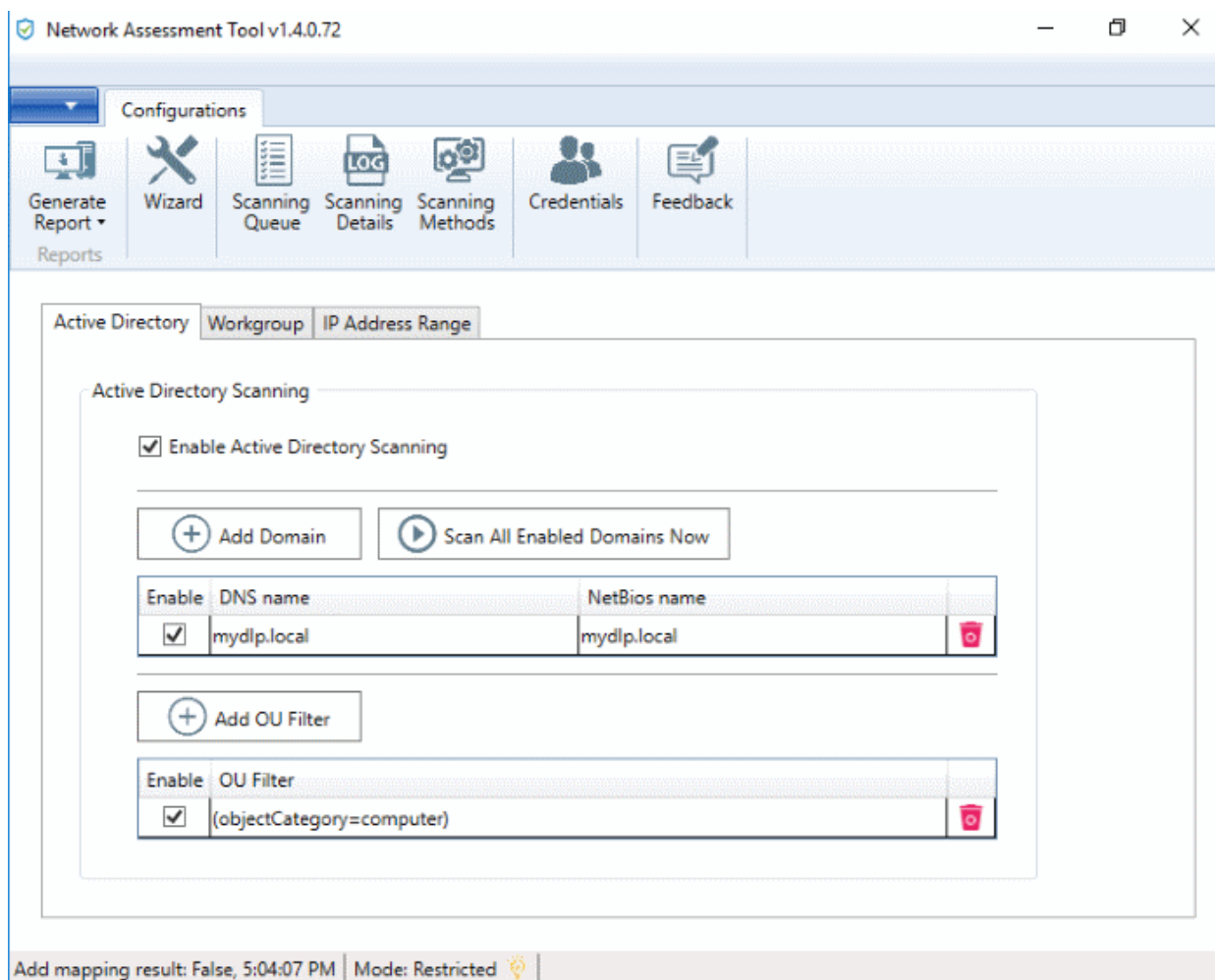
- To view scan progress, click the 'Scanning Queue' button
- To generate reports on completion of scan, click 'Generate Report'.

Step 4 - Add Networks

NAT allows you to add multiple target networks. You can add networks via Active Directory domain, by Workgroup or by IP range.

To add a network:

- Click 'Scanning Methods' on the menu bar:



- Select 'Active Directory', 'Workgroup' or 'IP Address Range' tab depending on the type you want to add.

Add an Active Directory domain

- Click the 'Active Directory' tab
- Make sure 'Enable Active Directory Scanning' is selected
- Click 'Add Domain'
- A new row will be added to the list
- Enter the DNS and NetBios names in the respective fields.

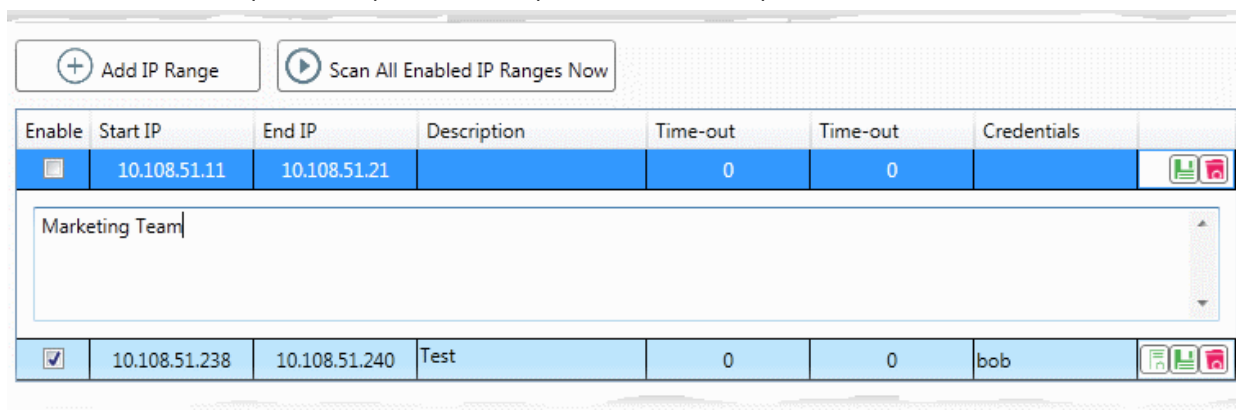
Add a workgroup



- Click the 'Workgroup' tab
- Make sure 'Enable Workgroup Scanning' is selected
- Click 'Add Workgroup'
- A new row will be added
- Enter the name of the workgroup you want to scan

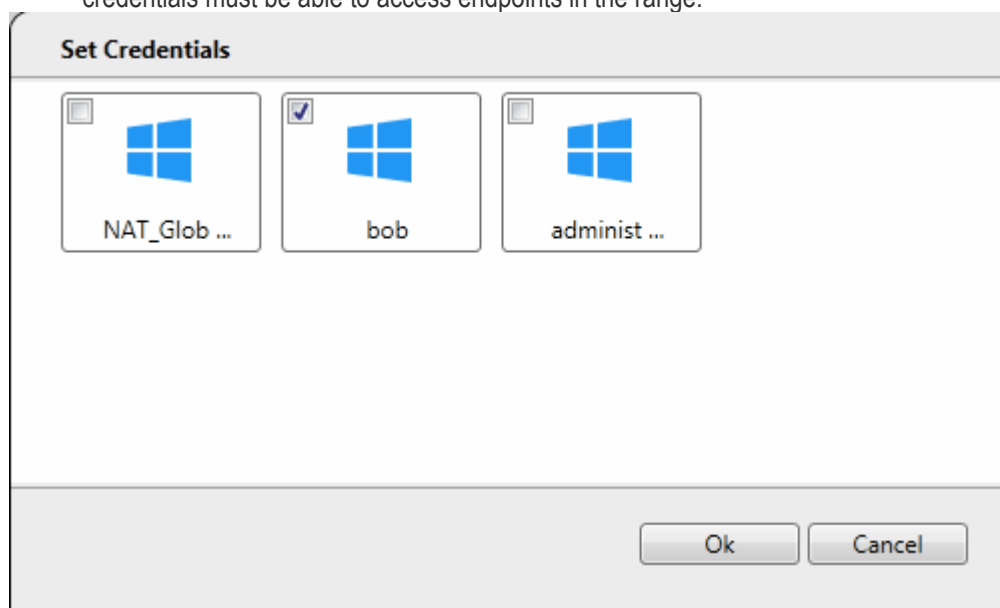
Add an IP Address Range

- Click the 'IP Address Range' tab
- Make sure 'Enable IP Address Range Scanning' is selected
- Click 'Add IP Range'
- A new row will be added to the list
- Enter the start and end IP addresses in the respective fields

- Enter a description for the IP range in the text-box
- Time out period - Skip scans on endpoints that do not respond in the set time.

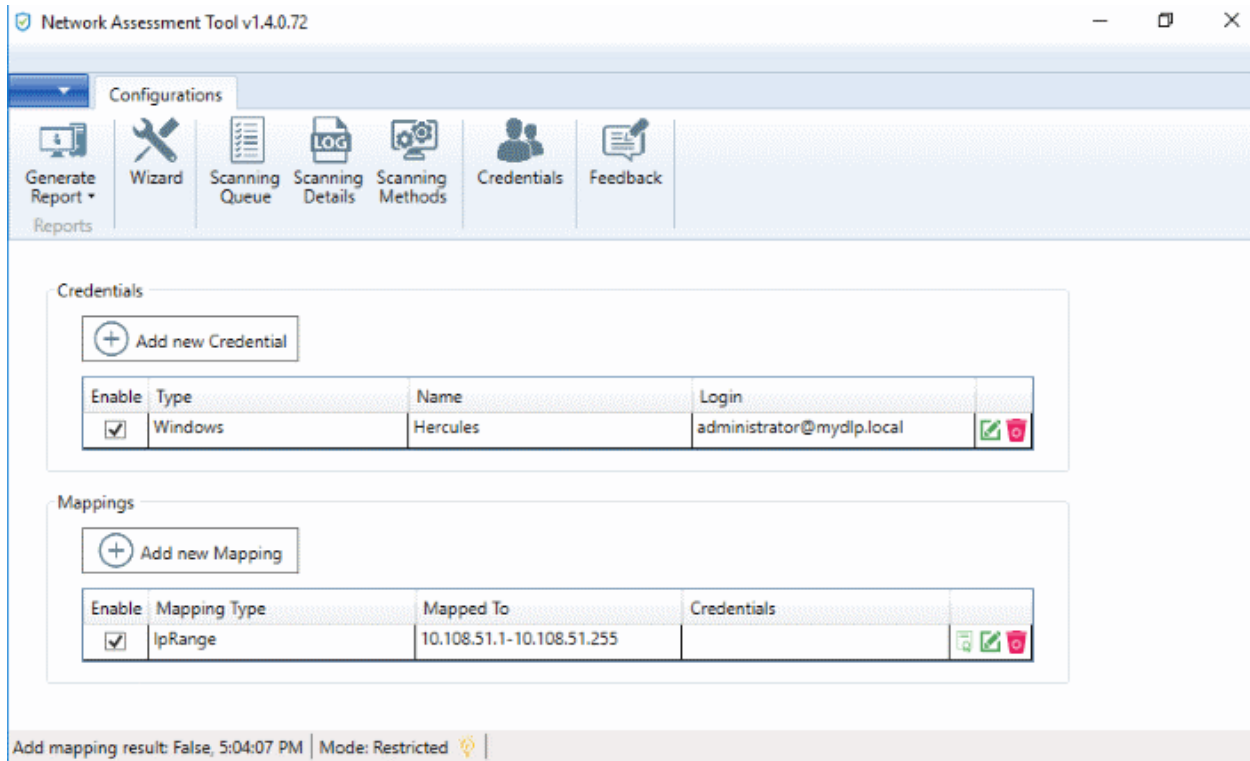


- Click the 'Save' button  to add the IP range. The next step is to map login credentials to the IP address range. NAT saves the credentials you entered during initial configuration.
 - Click the 'Credentials' button in the top-menu if you want to add more accounts. The next section, **Step 5 - Add Credentials and Map to Respective Networks**, offers help with this if you need it.
- Click the 'Add Credential' button  and select the logins you want to map to the IP range. All credentials must be able to access endpoints in the range.



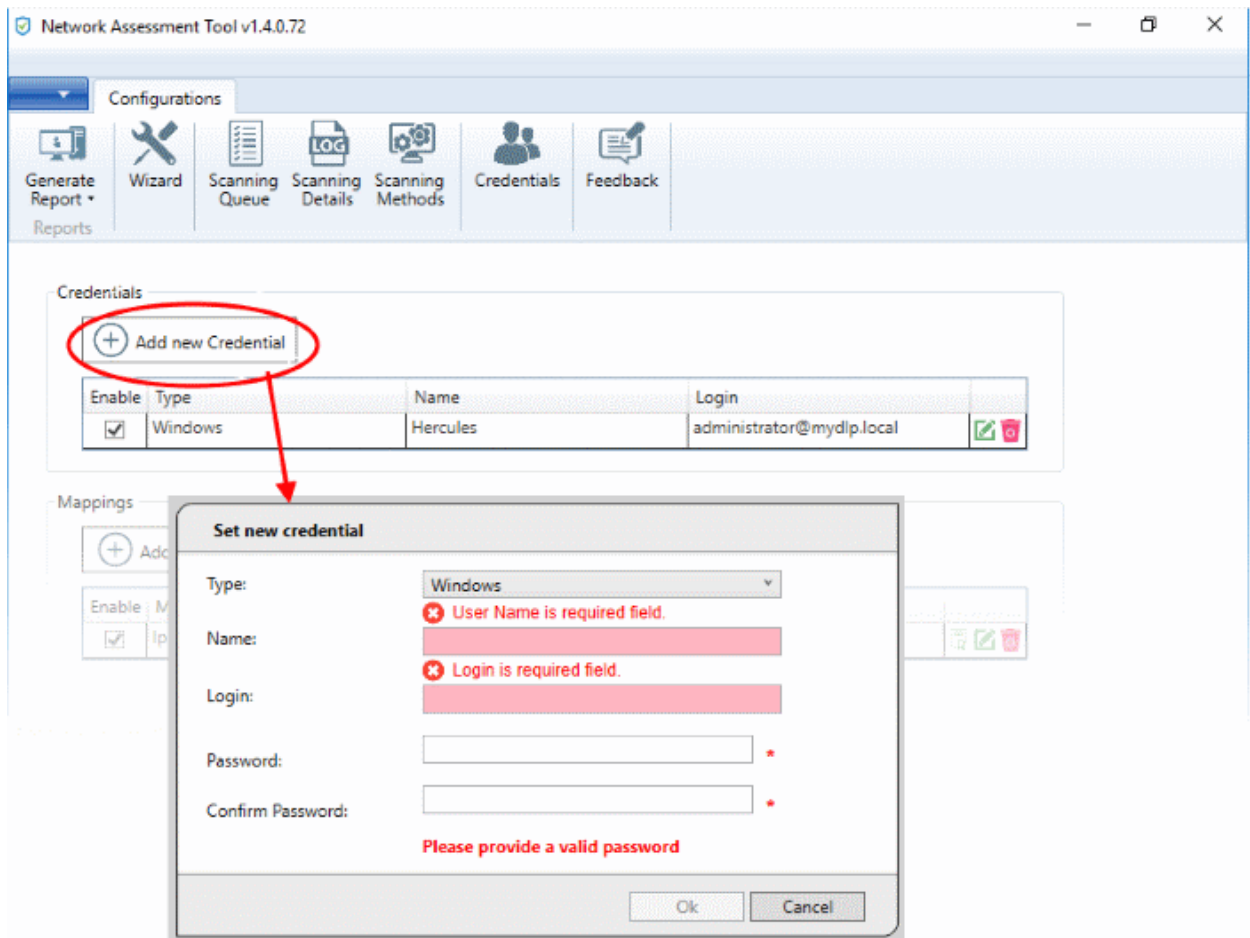
Step 5 - Add Credentials and Map to Respective Networks

- You need to provide admin username and password for target networks so NAT can scan their endpoints.
- You can map multiple credentials to a single network. NAT will try all credentials if one set fails on a particular endpoint.
- Click 'Credentials' on the menu bar to get started:



To add a new login credential

- click 'Add new Credential'



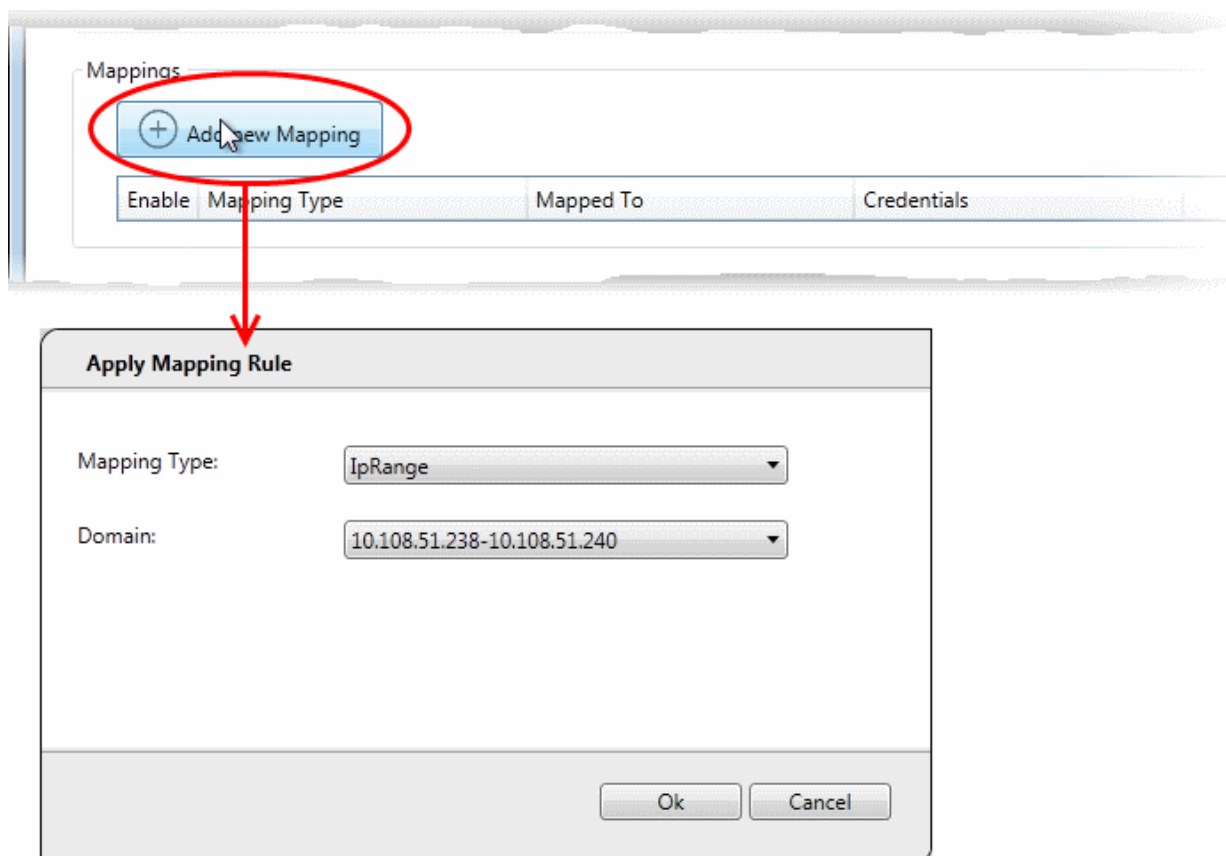
The 'Set new credential' dialog will open.

Set new credential dialog - Form parameters	
Form Element	Description
Type	Choose the operating system of the endpoints to which the credentials apply.
Name	A name to identify the account. For example, the name of the administrator
Login	The admin username
Password	The admin password

- Click 'OK' to add the credential
- Repeat the process to add more credentials

Map credentials to a network

- Click the 'Credentials' button in the top menu
- Click 'Add new Mapping' to open the wizard:

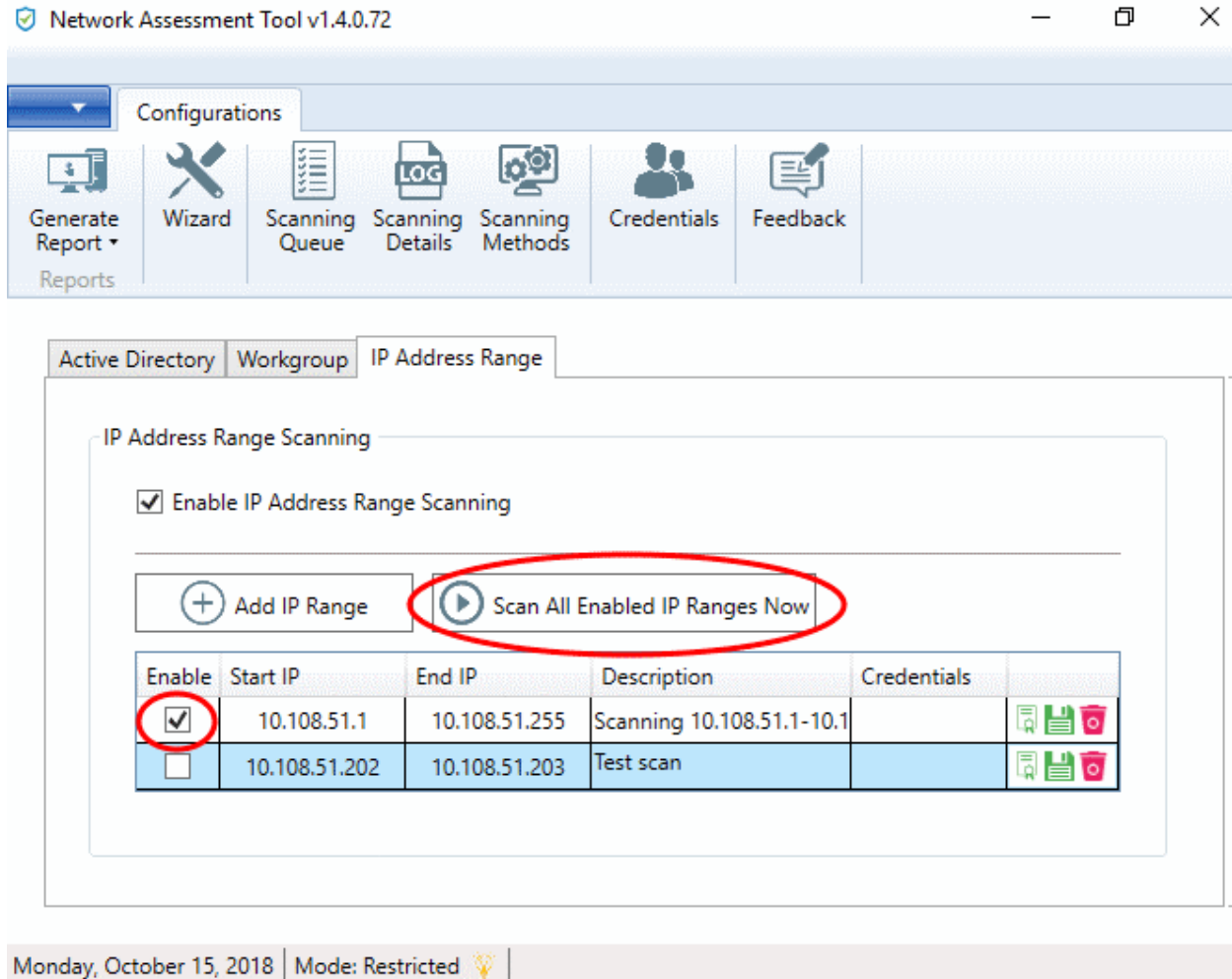


- Mapping Type - Choose the type of the network to which the credentials are to be mapped. The available choices are 'IP Range', 'Domain' and 'Workgroup'.
- Domain - The drop-down displays the networks added to NAT and fall under the type chosen from the 'Type' drop-down. Choose the network to which the credential is to be applied
- Click 'Ok'
- Repeat the process to map the credentials to different networks as needed

Step 6 - Run a Scan

- Click 'Scanning Methods' on the menu bar

- Click the tab of the type of network you want to scan - 'Active Directory', 'Workgroup', 'IP range'.
- Ensure the networks you want to scan are enabled. Disable those you do not want to scan.
- Click 'Scan All Enabled Domains/Workgroups/IP Ranges Now':



- The scan will start.
- Click the 'Scanning Queue' button to view scan progress:

Scanserver DESKTOP-TTPO9PR is running

Total scanned: 0

Scan service started at 10/15/2018 11:56:47 AM

Scanning Information

Discovery Type	IpRange	Credentials
IP Range	10.108.51.1-10.108.51.255	None

Stop scanning

IP Scanning

Processing: 3
In Queue: 232

Status	Target
🌀	10.108.51.22
🌀	10.108.51.23
🌀	10.108.51.21
➔	10.108.51.24
➔	10.108.51.25
➔	10.108.51.26
➔	10.108.51.27
➔	10.108.51.28

Windows computer scanning

Processing: 0
In Queue: 0

Status	Target
--------	--------

Monday, October 15, 2018 | Mode: Restricted | Discovering started... | 1 new notification

- **Scanning Information** - Details about current scans on domains, workgroups and IP addresses.
- **IP Scanning** - List of IP addresses discovered by Nmap on the current network.
- **Windows Computer Scanning** - Host-names and IP addresses that are currently being scanned using Windows Management Instrumentation (WMI) and Microsoft Baseline Security Analyzer (MBSA).

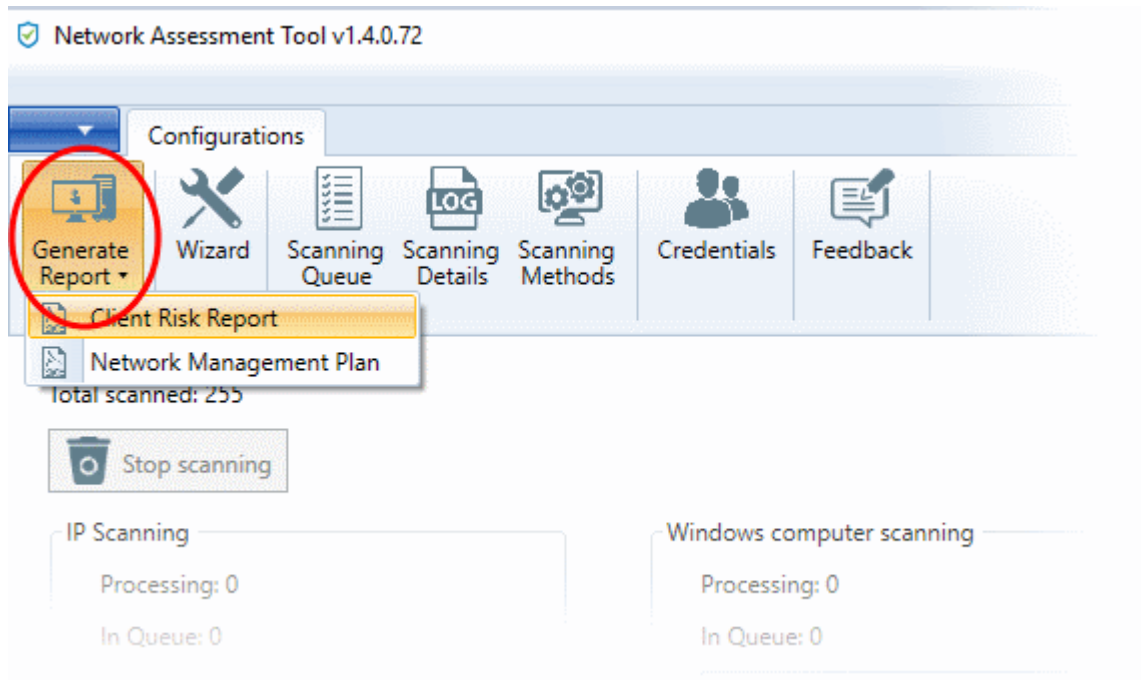
Step 7 - Generate Reports

There are two types of report you can generate after each scan:

- Client Risk Report – A breakdown of security issues on discovered network assets.
- Network Management Plan - Remediation advice for items listed in the risk report.

Download reports from the last scan

- Click 'Generate Report' from the menu bar
- Choose the report type from the drop-down



NAT will start generating the report and on completion you will be able to download and save the report on your computer.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: EnterpriseSolutions@Comodo.com