



**COMODO**  
Creating Trust Online®

**COMODO**  
**one**

# Comodo One

Software Version 3.26

---

## 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:

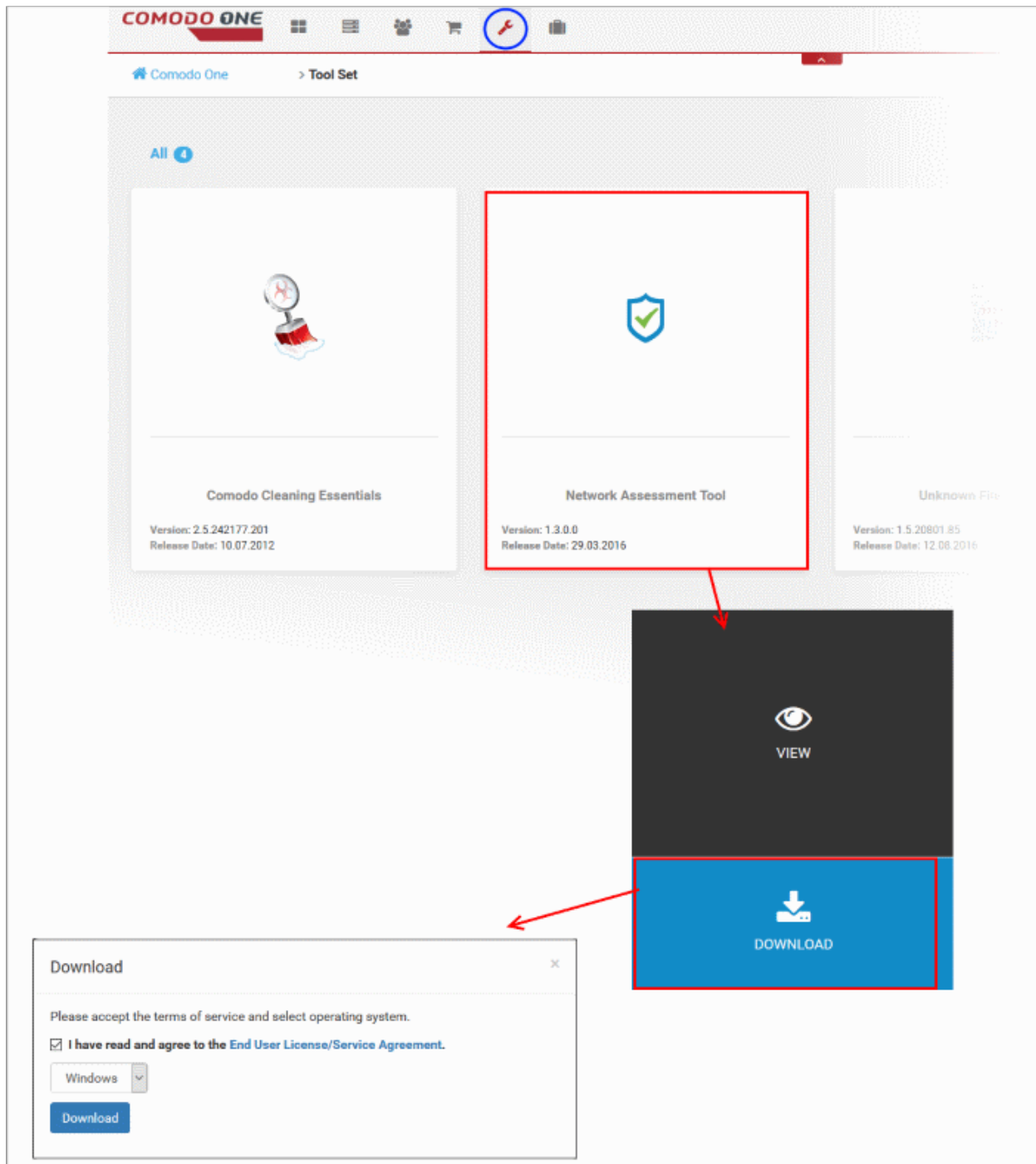
- Install the NAT tool and run the initial configuration wizard. The wizard allows you to enable scanning your domain/workgroup/IP Address Range, to which your computer is a member of and specify the administrative credentials for NAT to access the endpoints on your network.
- Add additional domains/workgroups/IP 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>.
- Once logged-in, click 'Tool Set' at the top.
- Hover your mouse over 'Network Assessment Tool' and click 'Download'



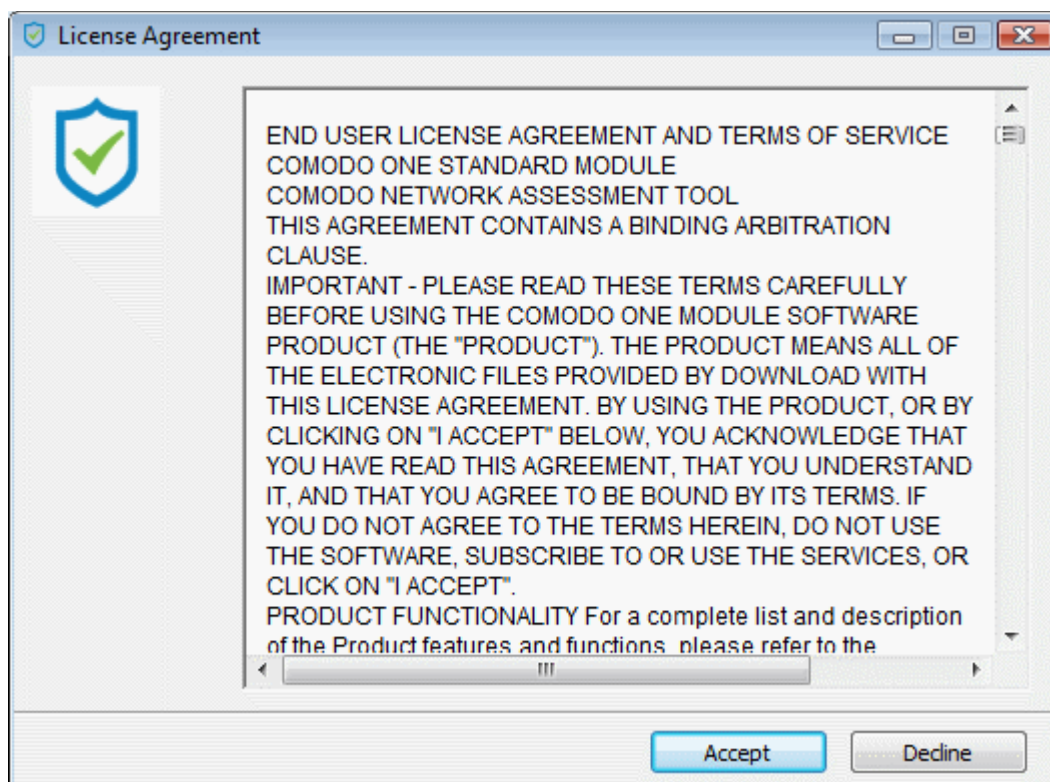
The 'Download' dialog will open.

- Click 'End User License/service Agreement', read the agreement and accept to it by selecting the EULA check box
- Click the 'Download' button to start the download of NAT setup file.

## 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.

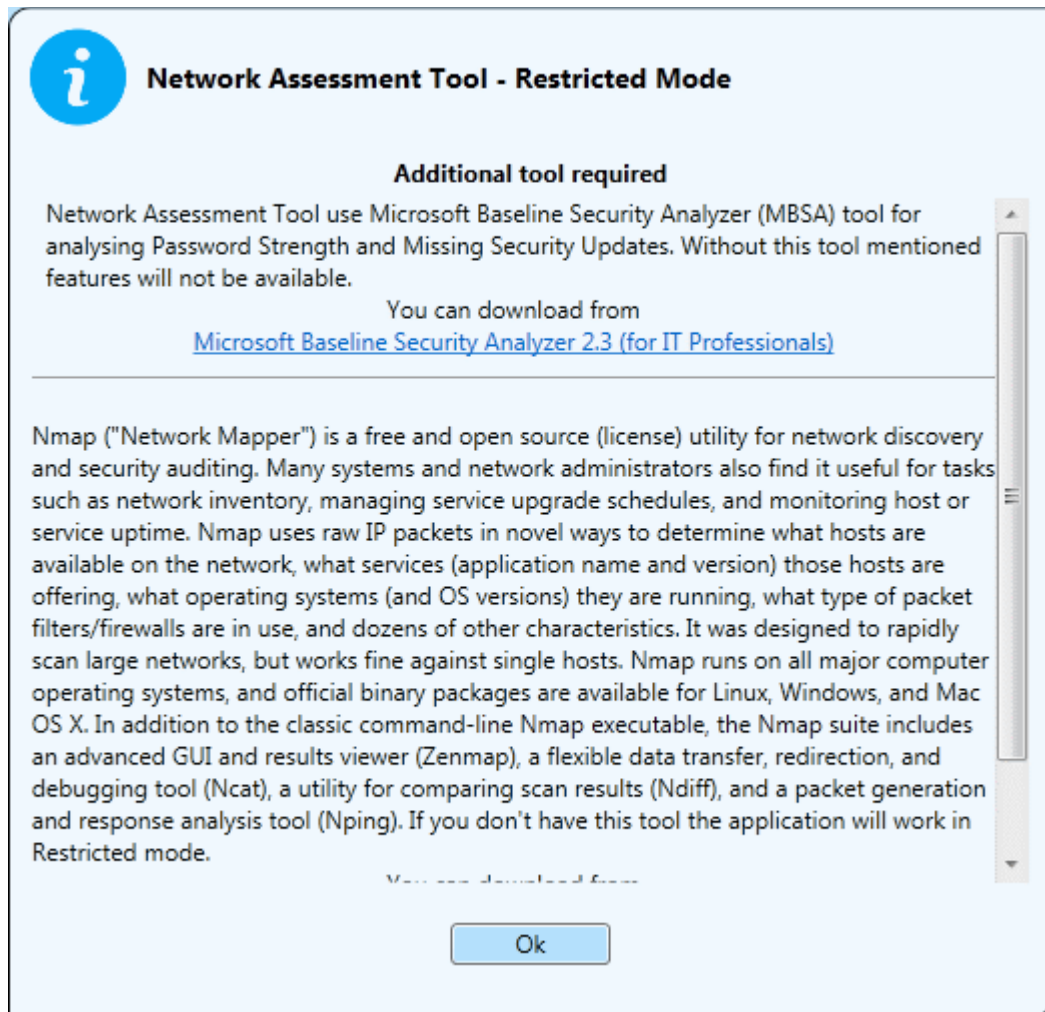
- Double click on the setup file  to start the NAT installation wizard



- Follow the wizard and continue the installation.

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

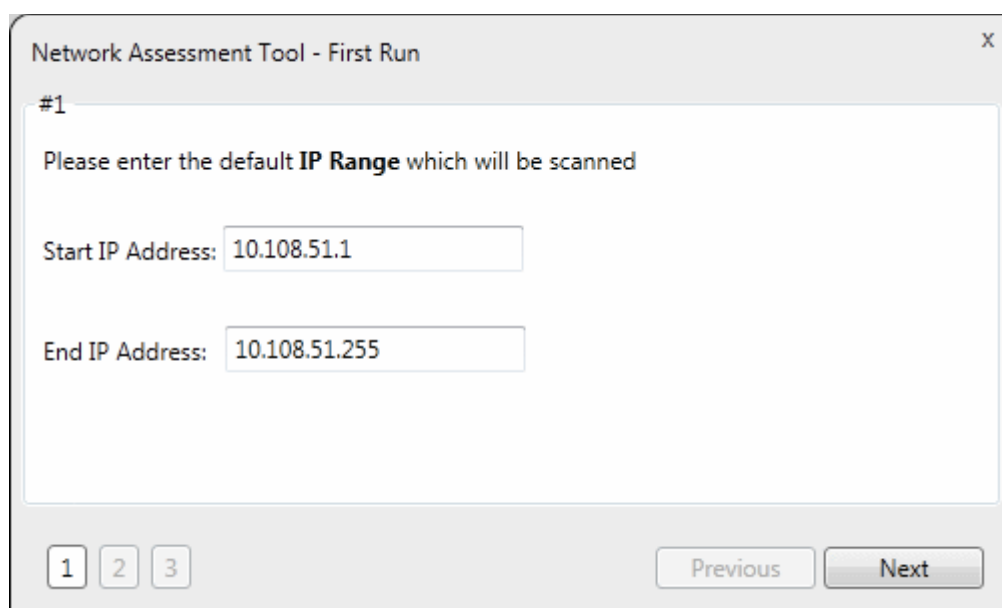
- If available, the installation will complete and will move to the **initial configuration wizard**.
- If not available a dialog containing guidance and download links for the additional software will be displayed.



- You can download and install the Nmap tool and MBSA tool by clicking the respective links in the dialog.

### Step 3 - Run Initial Configuration Wizard

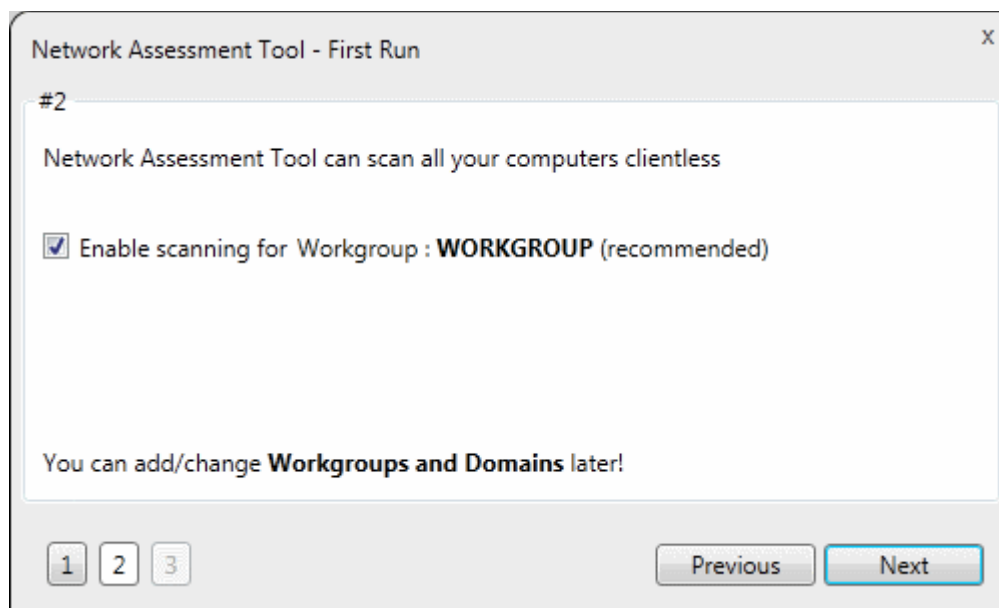
On completion of installation and if the Nmap tool and MBSA tool are available, the initial configuration wizard will begin.



NAT identifies the network on which it is installed and populates the 'Start IP Address' and 'End IP Address'

If required, you can change the Start and End IP Addresses of your network to be scanned. Also, you can add and manage networks to be scanned to NAT. Refer to the section **Network Management** for more details.

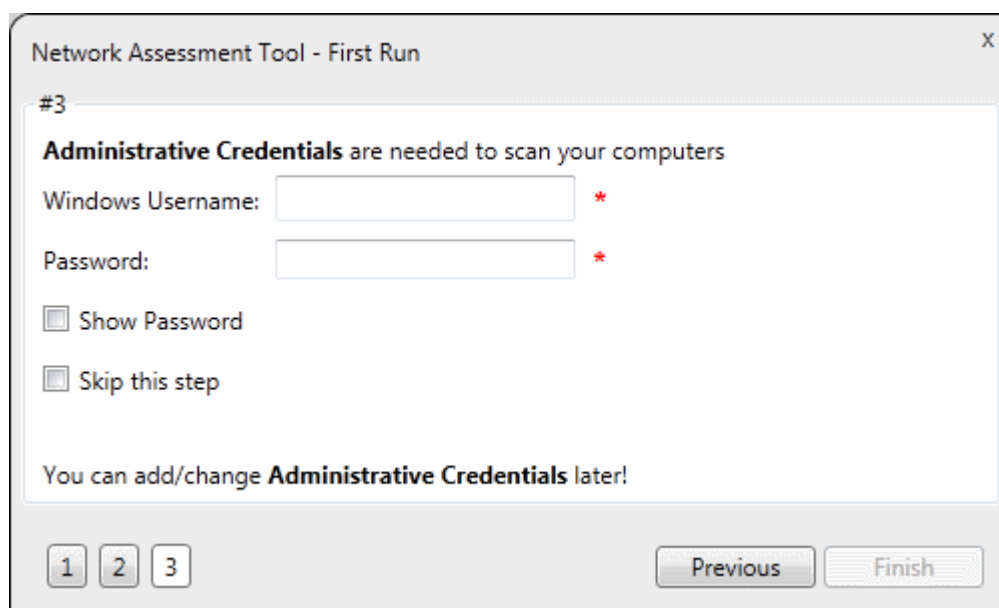
- Click 'Next' to move to the next step.



The screenshot shows a dialog box titled "Network Assessment Tool - First Run" with a close button (X) in the top right corner. The main content area contains the following text: "#2", "Network Assessment Tool can scan all your computers clientless", and a checked checkbox labeled "Enable scanning for Workgroup : **WORKGROUP** (recommended)". Below this, it says "You can add/change **Workgroups and Domains** later!". At the bottom, there are three numbered buttons (1, 2, 3) and two buttons labeled "Previous" and "Next".

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

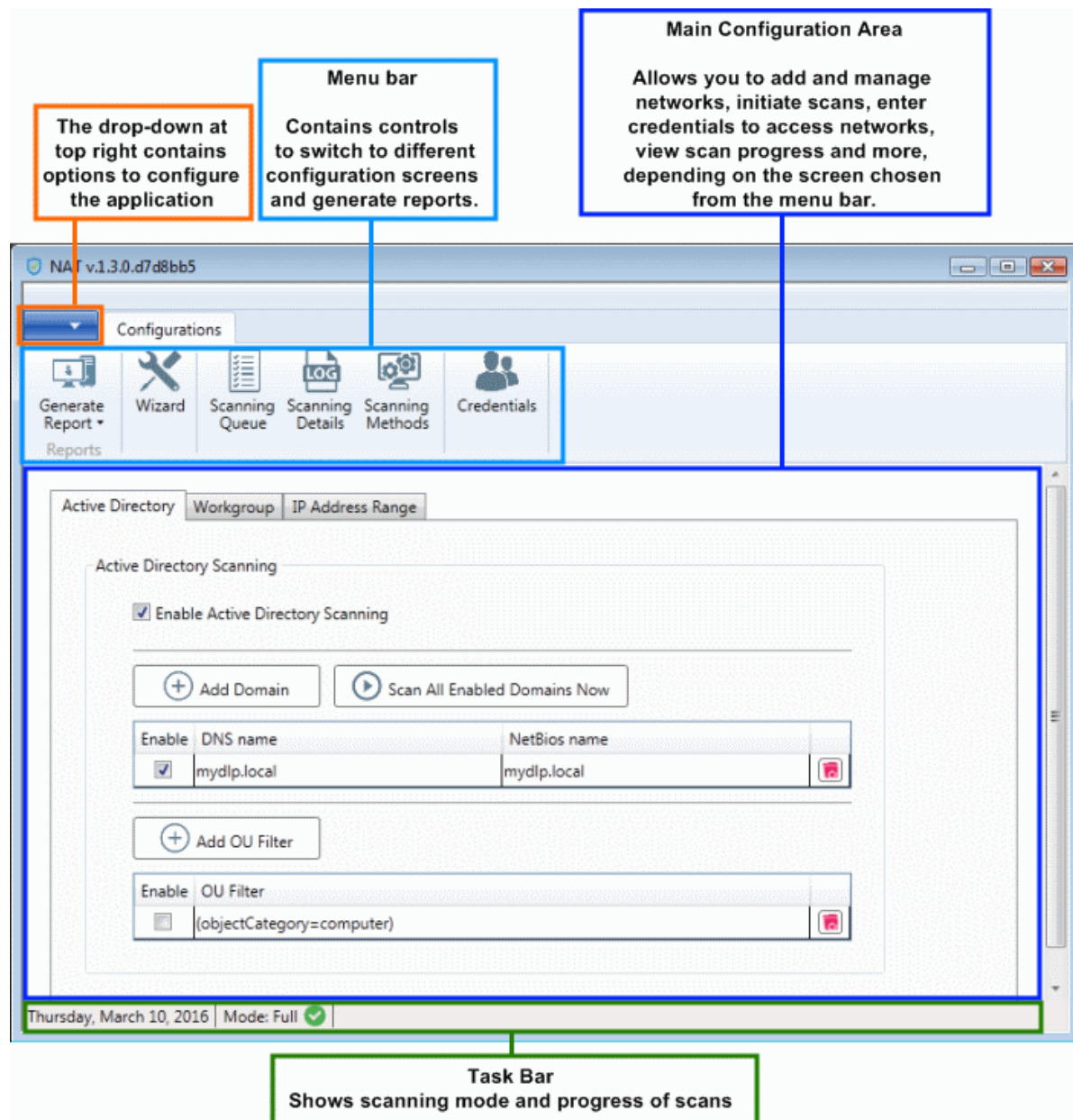
- To automatically add your workgroup/domain, ensure 'Enable scanning Workgroup/Domain' is selected and click 'Next'.



The screenshot shows a dialog box titled "Network Assessment Tool - First Run" with a close button (X) in the top right corner. The main content area contains the following text: "#3", "**Administrative Credentials** are needed to scan your computers", and two input fields: "Windows Username:" and "Password:", each followed by a red asterisk (\*). Below these are two checkboxes: "Show Password" and "Skip this step". At the bottom, it says "You can add/change **Administrative Credentials** later!". At the bottom left, there are three numbered buttons (1, 2, 3) and two buttons labeled "Previous" and "Finish".

- Enter an admin username and password for machines on the target network and click 'Finish'.
- NAT will immediately begin scanning your network and the main interface will open:



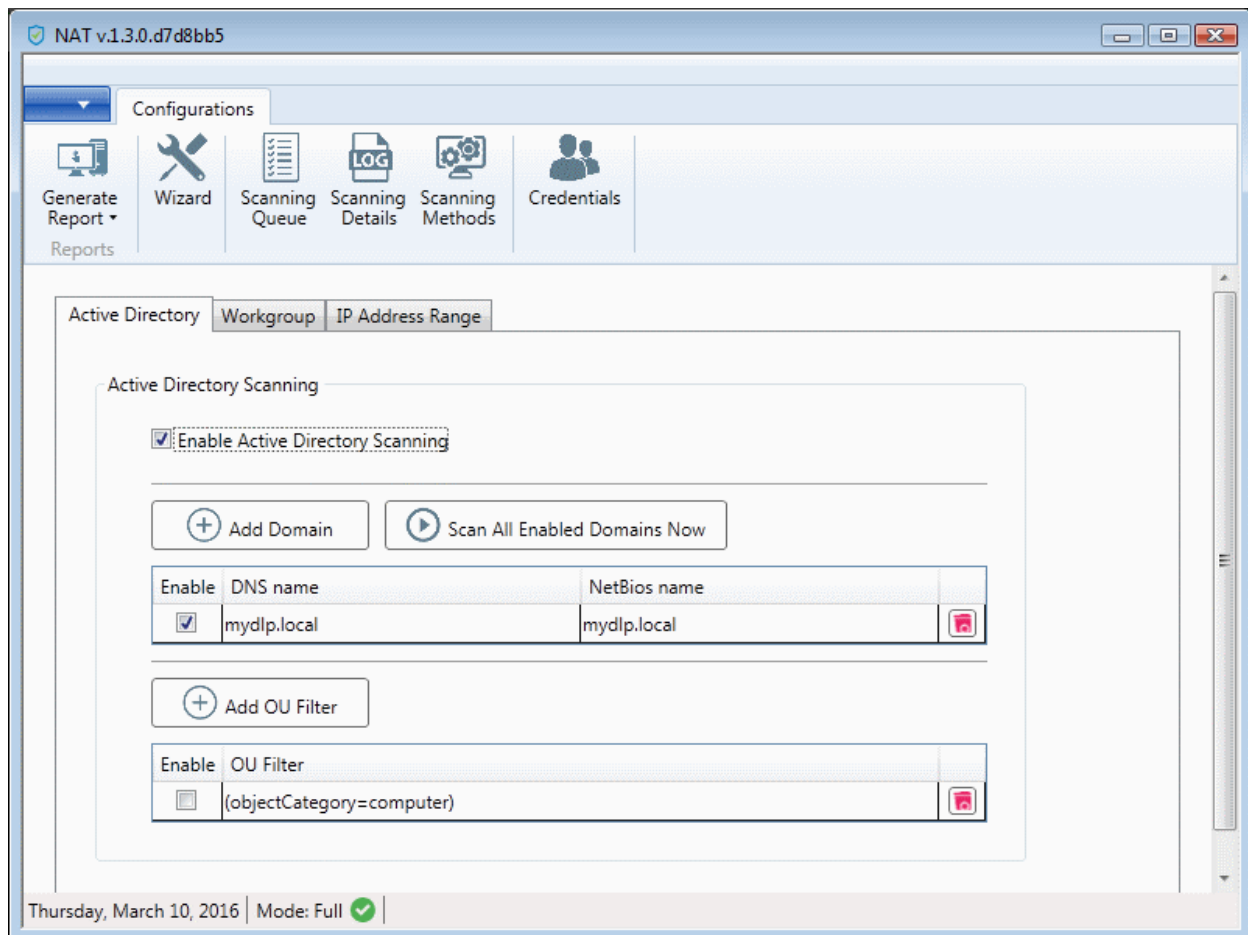


- To view scan progress, click the 'Scanning Queue' button
- To generate reports on completion of scan, click 'Generate Report'.

### Step 4 - Add Networks

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

- Click 'Scanning Methods' from the menu bar



- Select the any one of the tabs from 'Active Directory', 'Workgroup' and 'IP Address Range' depending on the network type you wish to add.

#### To add a domain

- Click the 'Active Directory' tab, ensure that the 'Enable Active Directory Scanning' check-box is selected and click 'Add Domain'  
A new row will be added to the list
- Enter the DNS name and NetBios name in the respective fields.

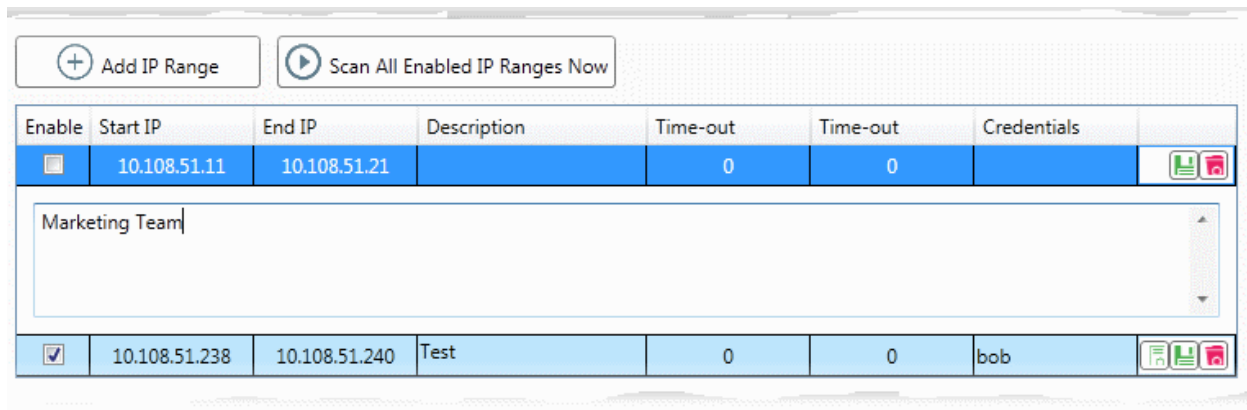
#### To add a workgroup

- Click the 'Workgroup' tab, ensure that the 'Enable Workgroup Scanning' check-box is selected and click 'Add Workgroup'  
A new row will be added to the list of workgroups.
- Enter the name of the workgroup to be added.

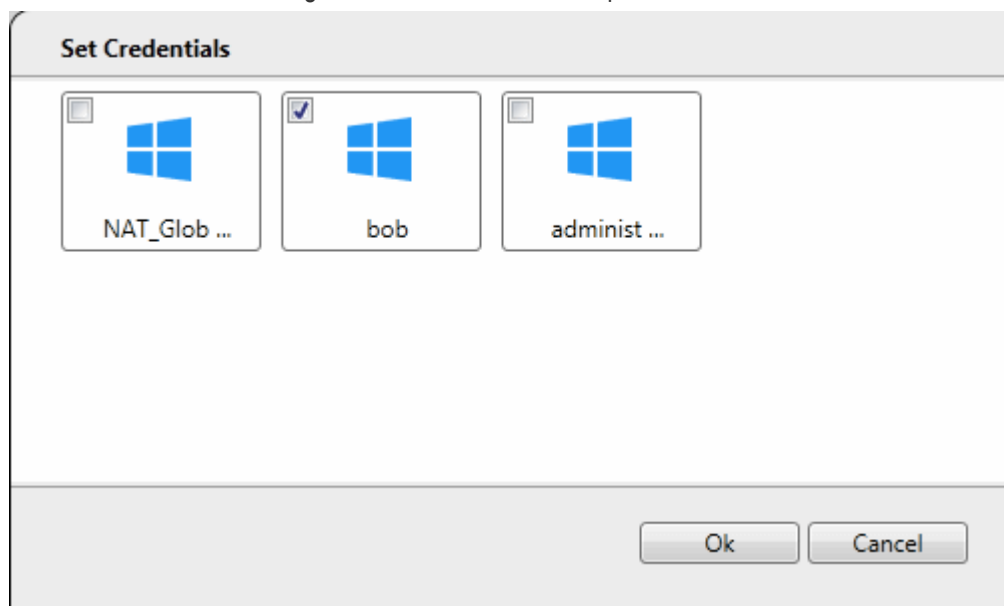
#### To add an IP Address Range

- Click the 'IP Address Range' tab, ensure that the 'Enable IP Address Range Scanning' check-box is selected and click 'Add IP Range'  
A new row will be added to the list of IP Address Ranges.
- Enter the start IP address and the end IP address in the respective fields
- Enter a description for the IP address range in the textbox that appears below the row.
- Enter the time out period for WMI so as to skip scanning the endpoints that are not responsive for the period specified in this field.





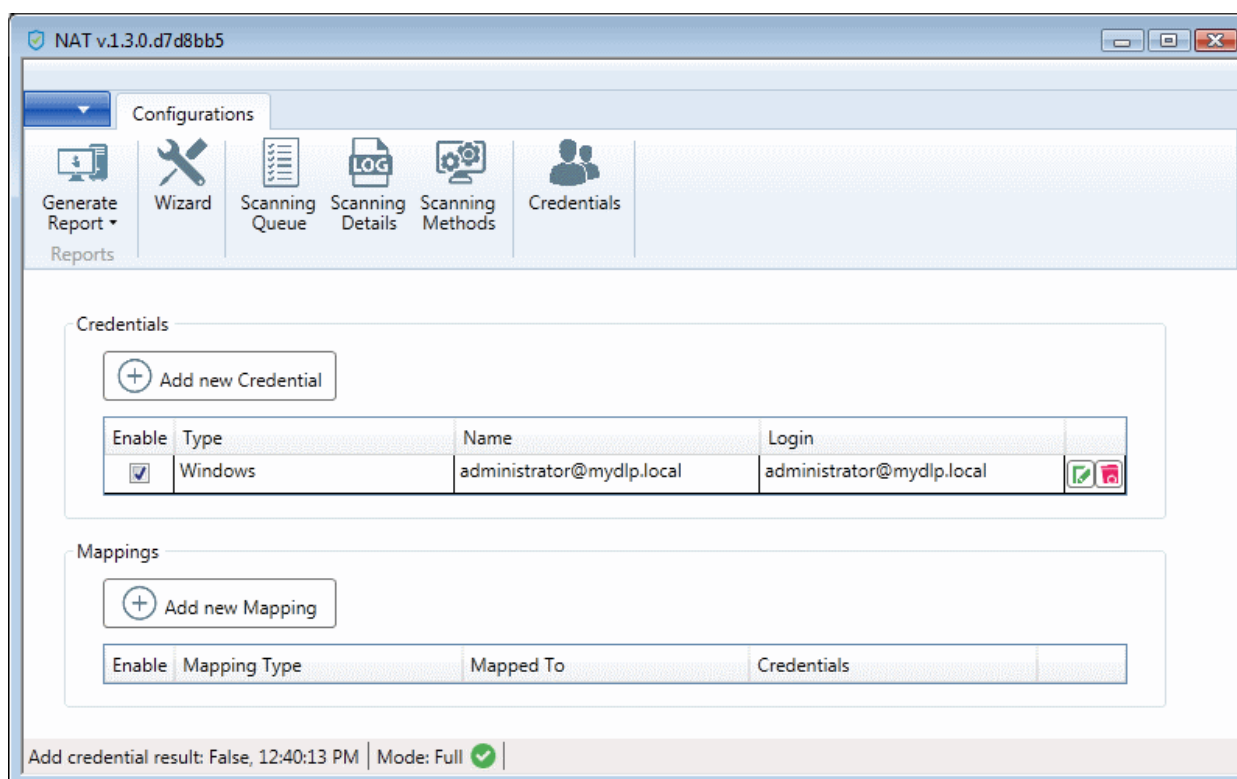
- Click the 'Save' button at the right of the row to add the IP address range. The next step is to map login credentials to the IP address range. NAT stores the credentials entered in the initial configuration wizard. You can add more credentials for different administrative accounts from the Credentials interface. Refer to **Step 5 - Add Credentials and Map to Respective Networks** for more details.
- Click the 'Add Credential' button at the right of the row and choose the credentials to be mapped to the IP address range. You can choose more than one credential, if different endpoints in the IP address range can be accessed with respective credentials.



### Step 5 - Add Credentials and Map to Respective Networks

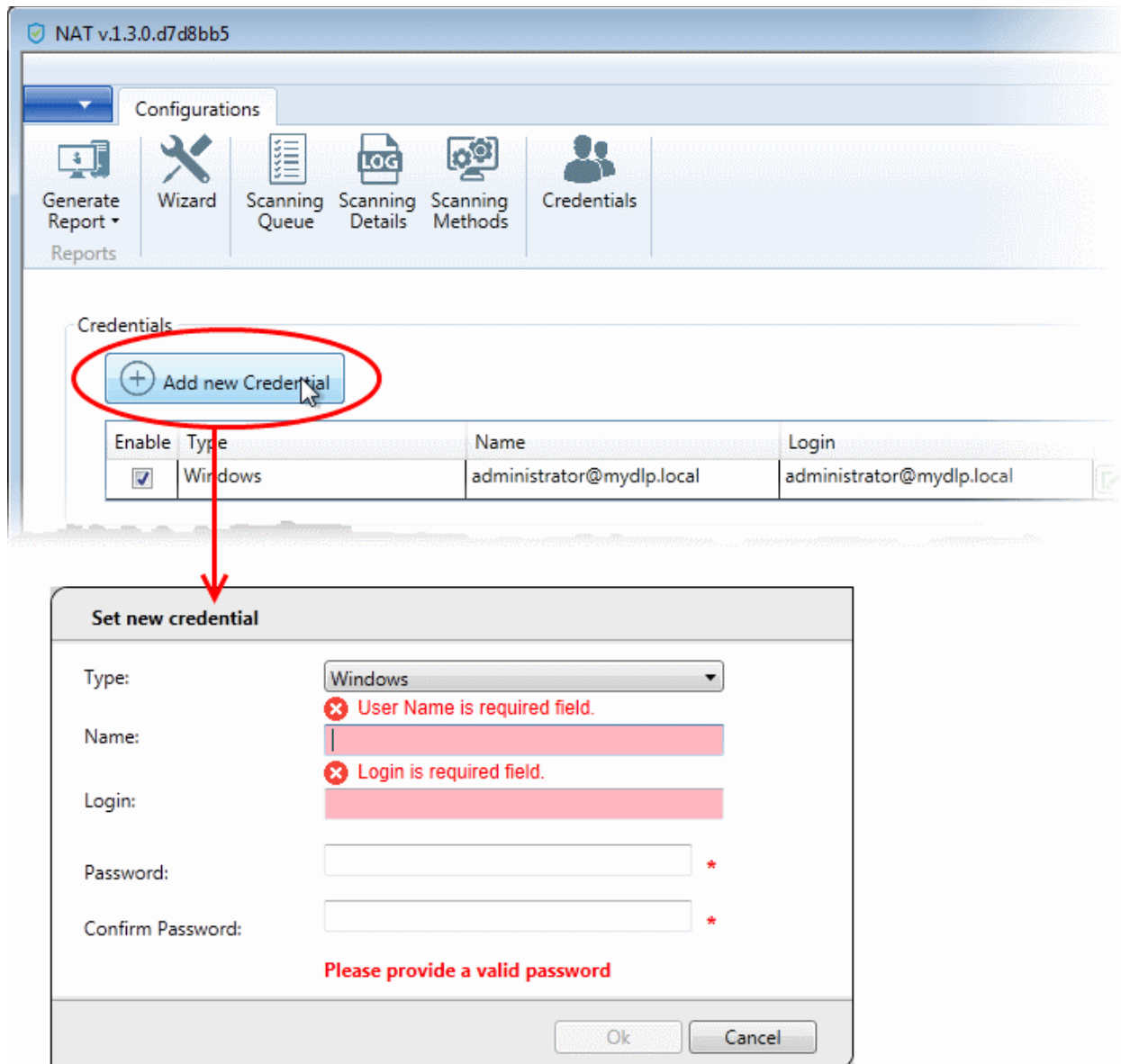
The next step is to add login credentials of network administrator accounts to NAT and map them to the networks, for NAT to access the endpoints in the scanned network(s). If different endpoints in a single network require different access credentials, you can add all the credentials and map them to the single network, so that , so that NAT can access each endpoint with the respective credential.

- Click 'Credentials' from the menu bar.



### To add a new login credential

- click 'Add new Credential'



The 'Set new credential' dialog will open.

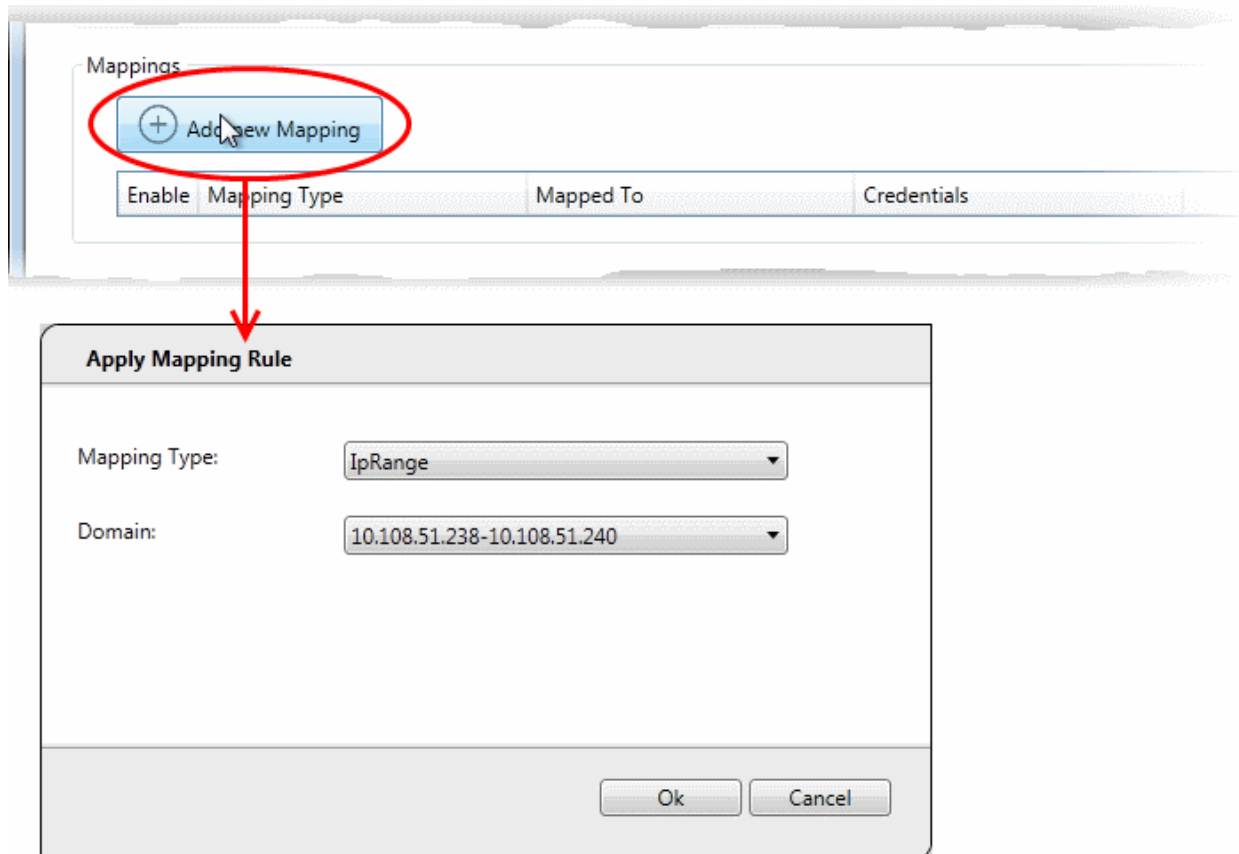
Set new credential dialog - Form parameters	
Form Element	Description
Type	Choose the operating system of the endpoints for which the credential is set
Name	Enter a name to identify the account, for example, the name of the administrator
Login	Enter the username of the account
Password	Enter the password of the account.
Confirm Password	Re-enter the password of confirmation

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

**To map credentials to a network**

- Click 'Add new Mapping' from the 'Credentials' interface

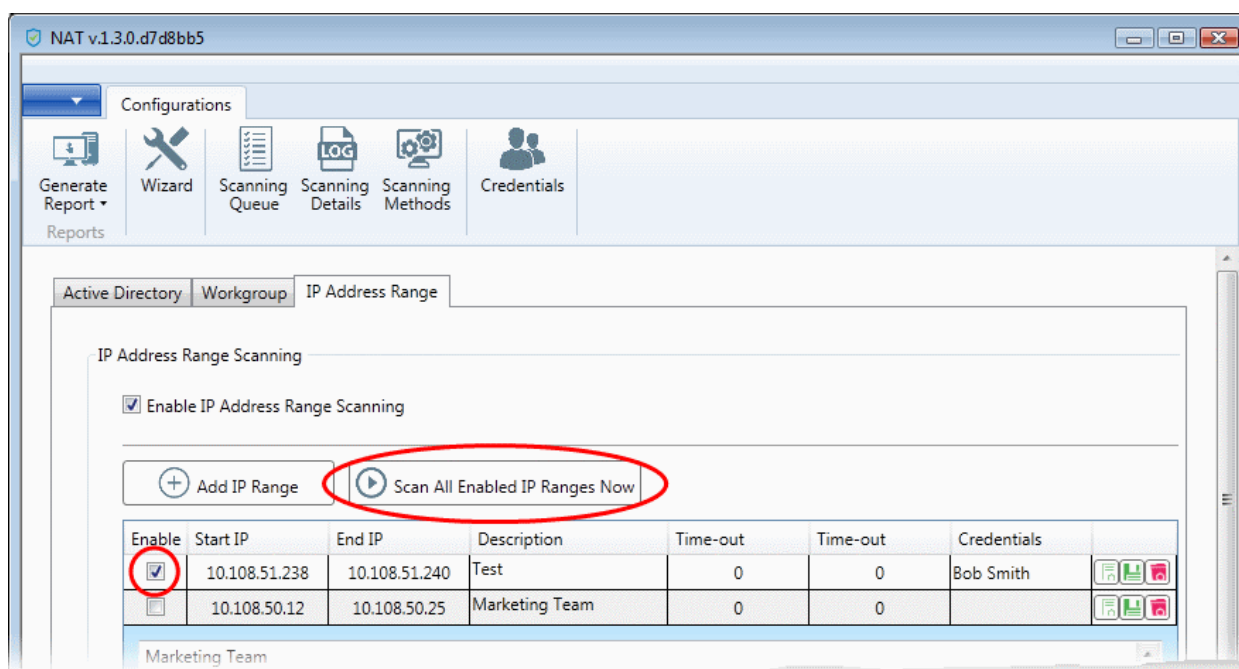
The 'Apply Mapping Rule' wizard will open.



- 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' from the menu bar
- Choose the type of network on which the scan is to be initiated, by selecting the respective tab.
  - Active Directory - To run the assessment scan on endpoints in a domain
  - Workgroup - To run the assessment scan on endpoints in a workgroup
  - IP Address Range - To run the assessment scan on endpoints that fall within the specified IP address range in the network
- Ensure that the network(s) to be scanned are enabled and those that need not be scanned are not enabled
- Click 'Scan All Enabled Domains Now', 'Scan All Enabled Workgroups Now' or 'Scan All Enabled IP Ranges Now' as appropriate to the network type chosen.



The scan will be started. You can view the progress of the scan from the 'Scanning Queue' interface.

- Click 'Scanning Queue' from the menu bar

The screenshot shows the NAT v.1.3.0.d7d8bb5 interface. At the top, there is a 'Configurations' menu with options: Generate Report, Wizard, Scanning Queue, Scanning Details, Scanning Methods, and Credentials. Below this, the status indicates 'Scanserver BOBSMITH-PC is running', 'Total scanned: 7', and 'Scan service started at 3/14/2016 5:30:49 PM'. A 'Scanning Information' table is displayed:

Discovery Type	IpRange	Credentials
IP Range	10.108.51.238-10.108.51.240	Bob Smith
IP Range	10.108.50.12-10.108.50.25	None

Below the table is a 'Stop scanning' button. The interface is divided into two main scanning sections: 'IP Scanning' and 'Windows computer scanning'. The 'IP Scanning' section shows 'Processing: 5' and 'In Queue: 0', with a table of targets:

Status	Target
🌞	10.108.50.21
🌞	10.108.50.22
🌞	10.108.50.23
🌞	10.108.50.24
🌞	10.108.50.25

The 'Windows computer scanning' section shows 'Processing: 0' and 'In Queue: 0', with a table containing headers 'Status' and 'Target'. At the bottom, a status bar shows 'Add credential result: False, 4:06:46 PM | Mode: Full | Assets scanning...' with a green progress bar.

- **Scanning Information** - Displays details about currently running scans on domain(s), Workgroup(s) and IP Address Range(s).
- **IP Scanning** - Displays the list of IP addresses discovered on the currently scanned network using Network Mapper (Nmap).
- **Windows Computer Scanning** - Displays a list of hostnames/IP addresses being scanned using Windows Management Instrumentation(WMI) and Microsoft Baseline Security Analyzer (MBSA)
- To terminate the scan, click 'Stop Scanning'.

The successful completion of scanning will be indicated.

### Step 7 - Generate Reports

You can generate assessment reports after the completion of each scan.

NAT can generate two types of reports:

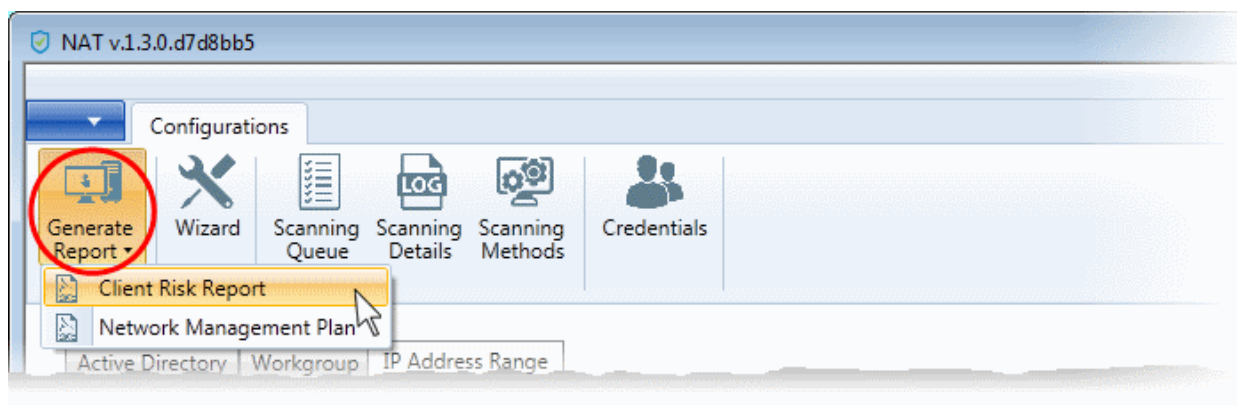
- **Client Risk Report** - Contains details on discovery scans performed on the network, details on network assets, issues identified, storage status on the discovered endpoints and more.



- Network Management Plan - Contains remediation advice for items listed in the risk report..

#### To 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](mailto:EnterpriseSolutions@Comodo.com)